

# Дискреционное разграничение прав в Linux. Основные атрибуты

---

Александр Дмитриев<sup>1</sup>

13 сентября, 2023, Москва, Россия

<sup>1</sup>Российский Университет Дружбы Народов

# Цели и задачи работы

---

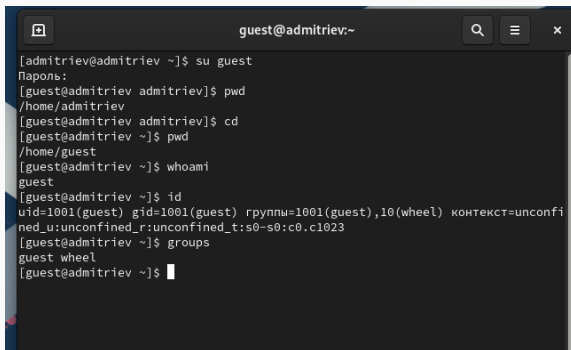
## Цель лабораторной работы

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**

---

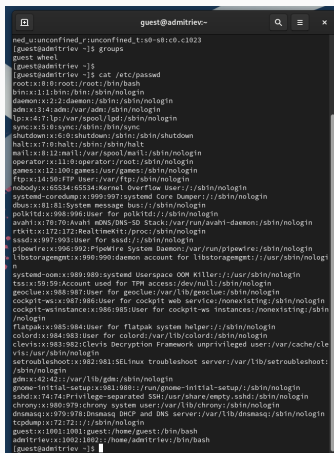
# Определяем UID и группу

A terminal window titled 'guest@admitriev:~' with search, menu, and close icons in the title bar. The terminal shows a sequence of commands and their outputs: 'su guest' (password prompt), 'pwd' (returns /home/admitriev), 'cd' (returns /home/guest), 'whoami' (returns guest), 'id' (returns uid=1001(guest) gid=1001(guest) rгруппы=1001(guest),10(wheel) контекст=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023), and 'groups' (returns guest wheel).

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

**Figure 1:** Информация о пользователе guest

# Файл с данными о пользователях



```
guest@admitriev:~  
red_unconfined_r:unconfined_t:s0-s0:c0.c1023  
(guest@admitriev ~) $ groups  
guest wheel  
(guest@admitriev ~) $  
(guest@admitriev ~) $ 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:5:8: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: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:907:903: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  
n  
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:907:906:User for cockpit web service:/nonexistent:/sbin/nologin  
cockpit-ws-instance:x:986:985:User for cockpit-ws instances:/nonexistent:/sbin/nologin  
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:/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  
crpdump:x:172:172:/sbin/nologin  
guest:x:1001:1001:guest:/home/guest:/bin/bash  
admitriev:x:1002:1002:/home/admitriev:/bin/bash  
(guest@admitriev ~) $
```

Figure 2: Содержимое файла /etc/passwd

# Доступ к домашним директориям

```
[guest@admitriev ~]$  
[guest@admitriev ~]$ ls -l /home  
итого 8  
drwx-----, 14 admitriev admitriev 4096 сен 13 11:43 admitriev  
drwx-----, 14 guest      guest      4096 сен 13 11:52 guest  
[guest@admitriev ~]$
```

Figure 3: Расширенные атрибуты

# Атрибуты директории

```
[guest@admitriev ~]$  
[guest@admitriev ~]$ cd  
[guest@admitriev ~]$ mkdir dir1  
[guest@admitriev ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 сен 13 12:04 dir1  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Видео  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Документы  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Загрузки  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Изображения  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Музыка  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Общедоступные  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 'Рабочий стол'  
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Шаблоны  
[guest@admitriev ~]$ chmod 000 dir1/  
[guest@admitriev ~]$ ls -l dir1/  
ls: невозможно открыть каталог 'dir1/': Отказано в доступе  
[guest@admitriev ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@admitriev ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@admitriev ~]$
```

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.