

Дискреционное разграничение прав в Linux. Основные атрибуты

Alexey A. Shemyakin¹

02 September, 2021 Moscow, Russian Federation

¹RUDN University, Moscow, Russian Federation

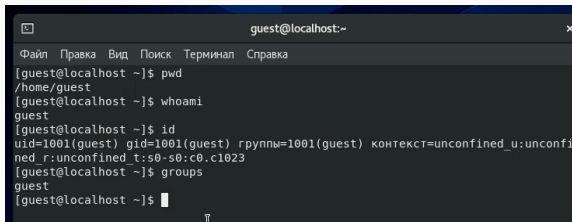
Цели и задачи работы

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

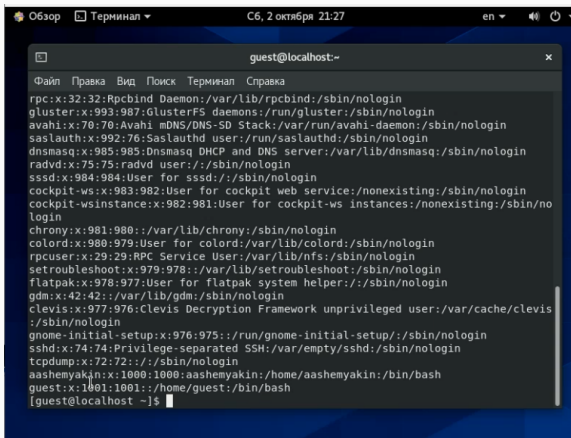
Определяем UID и группу



```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$ whoami  
guest  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$ groups  
guest  
[guest@localhost ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

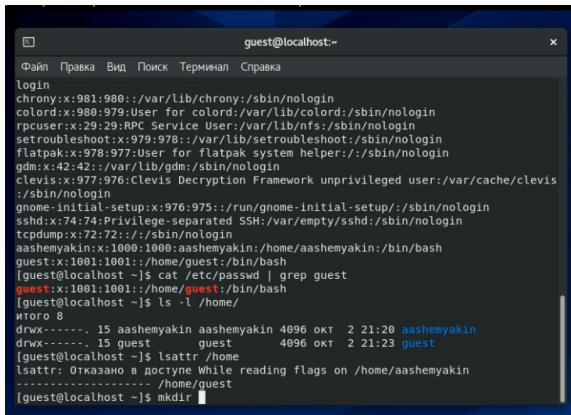


The image shows a terminal window titled "Обзор Терминал" with a timestamp of "С6, 2 октября 21:27". The terminal is running a command to display the contents of the `/etc/passwd` file. The output lists system users and regular users, each with their username, UID, GID, name, home directory, and shell. The prompt is `guest@localhost:~`.

```
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
gluster:x:993:987:GlusterFS daemons:/run/gluster:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
saslauth:x:992:76:Saslauthd user:/run/saslauthd:/sbin/nologin
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/sbin/nologin
sssd:x:984:984:User for sssd:/sbin/nologin
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
chrony:x:981:980:./var/lib/chrony:/sbin/nologin
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot:x:979:978:./var/lib/setroubleshoot:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
gnome-initial-setup:x:976:975:./run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:./sbin/nologin
aashemyakin:x:1000:1000:aashemyakin:/home/aashemyakin:/bin/bash
guest:x:1001:1001:./home/guest:/bin/bash
[guest@localhost ~]$
```

Figure 2: Содержимое файла `/etc/passwd`

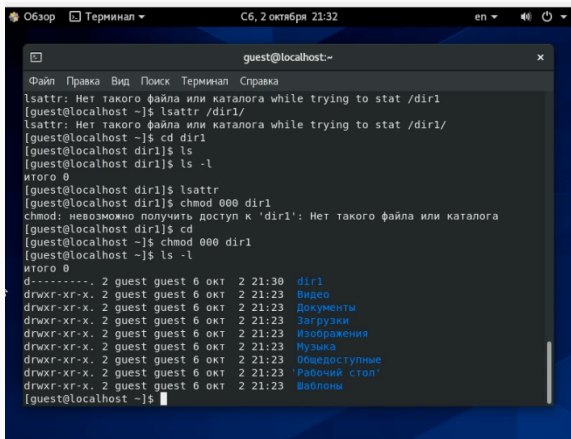
Доступ к домашним директориям



```
guest@localhost:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
login  
chrony:x:981:980::/var/lib/chrony:/sbin/nologin  
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
setroubleshoot:x:979:978::/var/lib/setroubleshoot:/sbin/nologin  
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis  
:/sbin/nologin  
gnome-initial-setup:x:976:975:/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
aashemyakin:x:1000:1000:aashemyakin:/home/aashemyakin:/bin/bash  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@localhost ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@localhost ~]$ ls -l /home/  
итого 8  
drwx----- 15 aashemyakin aashemyakin 4096 окт  2 21:20 aashemyakin  
drwx----- 15 guest      guest      4096 окт  2 21:23 guest  
[guest@localhost ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/aashemyakin  
----- /home/guest  
[guest@localhost ~]$ mkdir
```

Figure 3: Расширенные атрибуты

Атрибуты директории



The screenshot shows a terminal window titled "Обзор Терминал" with a timestamp of "Сб, 2 октября 21:32". The user is logged in as "guest" on "localhost". The terminal output shows the following sequence of commands and results:

```
lsattr: Нет такого файла или каталога while trying to stat /dir1
[guest@localhost ~]$ lsattr /dir1/
lsattr: Нет такого файла или каталога while trying to stat /dir1/
[guest@localhost ~]$ cd dir1
[guest@localhost dir1]$ ls
[guest@localhost dir1]$ ls -l
итого 0
[guest@localhost dir1]$ lsattr
[guest@localhost dir1]$ chmod 000 dir1
chmod: невозможно получить доступ к 'dir1': Нет такого файла или каталога
[guest@localhost dir1]$ cd
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d-----x. 2 guest guest 6 окт  2 21:30  dir1
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  Видео
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  Документы
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 21:23  Шаблоны
[guest@localhost ~]$
```

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.

Спасибо за внимание!