

Дискреционное разграничение прав в Linux. Основные атрибуты

Князьков Геннадий НБИ-01-19¹

13 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

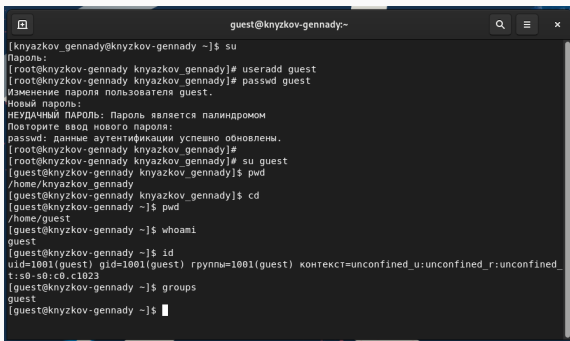
Цели и задачи работы

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

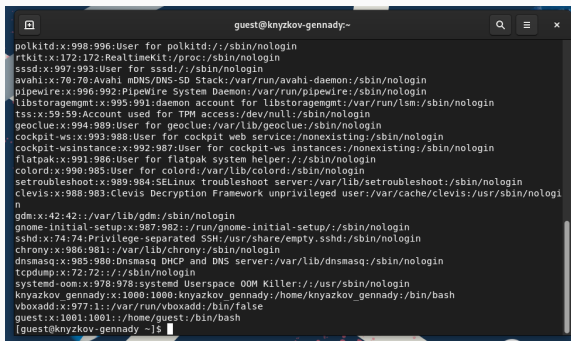
Определяем UID и группу



```
guest@knyzkov-gennady:~  
[knyazkov_gennady@knyzkov-gennady ~]$ su  
Пароль:  
[root@knyzkov-gennady knyazkov_gennady]# useradd guest  
[root@knyzkov-gennady knyazkov_gennady]# passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[root@knyzkov-gennady knyazkov_gennady]#  
[root@knyzkov-gennady knyazkov_gennady]# su guest  
[guest@knyzkov-gennady knyazkov_gennady]$ pwd  
/home/knyazkov_gennady  
[guest@knyzkov-gennady knyazkov_gennady]$ cd  
[guest@knyzkov-gennady ~]$ pwd  
/home/guest  
[guest@knyzkov-gennady ~]$ whoami  
guest  
[guest@knyzkov-gennady ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_  
t:s0-s0:c0.c1023  
[guest@knyzkov-gennady ~]$ groups  
guest  
[guest@knyzkov-gennady ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@knyazkov-gennady:~' displays the output of the 'cat /etc/passwd' command. The output lists system and regular users with their IDs, names, and shell paths. The window has a dark background and standard terminal icons in the title bar.

```
guest@knyazkov-gennady:~  
polkitd:x:998:996:User for polkitd:/:sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
sssd:x:997:993:User for sssd:/:sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin  
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin  
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin  
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin  
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin  
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin  
flatpak:x:991:986:User for flatpak system helper:/:sbin/nologin  
colord:x:990:985:User for colord:/var/lib/colord:/sbin/nologin  
setroubleshoot:x:989:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin  
clevis:x:988:983:clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin  
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:987:982:/:run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin  
chrony:x:986:981:/:var/lib/chrony:/sbin/nologin  
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
tcpdump:x:72:72:/:sbin/nologin  
systemd-oom:x:978:978:systemd Userspace OOM Killer:/:usr/sbin/nologin  
knyazkov_gennady:x:1000:1000:knyazkov_gennady:/home/knyazkov_gennady:/bin/bash  
vboxadd:x:977:1:/:var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@knyazkov-gennady ~]$
```

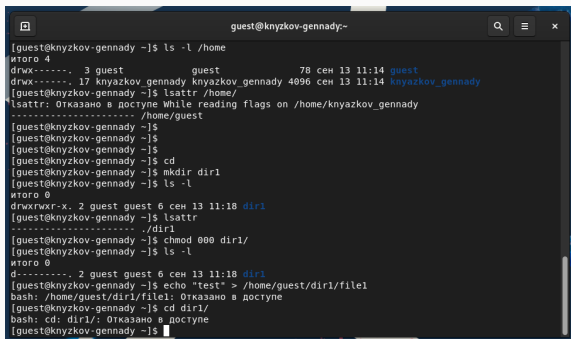
Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@knyzkov-gennady ~]$  
[guest@knyzkov-gennady ~]$  
[guest@knyzkov-gennady ~]$ ls -l /home  
иторо 4  
drwx-----, 3 guest          guest          78 сен 13 11:14 guest  
drwx-----, 17 knyazkov gennady knyazkov gennady 4096 сен 13 11:14 knyazkov_gennady  
[guest@knyzkov-gennady ~]$ lsattr /home/  
lsattr: Отказано в доступе While reading flags on /home/knyazkov_gennady  
----- /home/guest  
[guest@knyzkov-gennady ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@knyzkov-gennady~' showing a series of commands and their outputs. The user first runs 'ls -l /home', which shows a directory listing for '/home/guest'. Then, they run 'lsattr /home/' and receive an error: 'lsattr: Отказано в доступе While reading flags on /home/knyazkov_gennady'. Next, they run 'cd /home/guest' and then 'mkdir dir1'. After running 'ls -l', they see a new directory 'dir1'. Then, they run 'chmod 000 dir1/'. Finally, they run 'ls -l' again, showing 'dir1' with permissions 'd-----'. The last command is 'echo "test" > /home/guest/dir1/file1', which results in a 'bash: /home/guest/dir1/file1: Отказано в доступе' error. The prompt returns to the user's shell.

```
guest@knyzkov-gennady ~]$ ls -l /home
итого 4
drwx-----, 3 guest          guest          78 сен 13 11:14 guest
drwx-----, 17 knyazkov_gennady knyazkov_gennady 4096 сен 13 11:14 knyazkov_gennady
[guest@knyzkov-gennady ~]$ lsattr /home/
lsattr: Отказано в доступе While reading flags on /home/knyazkov_gennady
----- /home/guest
[guest@knyzkov-gennady ~]$
[guest@knyzkov-gennady ~]$
[guest@knyzkov-gennady ~]$
[guest@knyzkov-gennady ~]$ cd
[guest@knyzkov-gennady ~]$ mkdir dir1
[guest@knyzkov-gennady ~]$ ls -l
итого 0
drwxrwxr-x, 2 guest guest 6 сен 13 11:18 dir1
[guest@knyzkov-gennady ~]$ lsattr
----- ./dir1
[guest@knyzkov-gennady ~]$ chmod 000 dir1/
[guest@knyzkov-gennady ~]$ ls -l
итого 0
d-----, 2 guest guest 6 сен 13 11:18 dir1
[guest@knyzkov-gennady ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@knyzkov-gennady ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@knyzkov-gennady ~]$
```

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.