

Дискреционное разграничение прав в Linux. Основные атрибуты

Кеан Путхеаро¹

12 сентября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

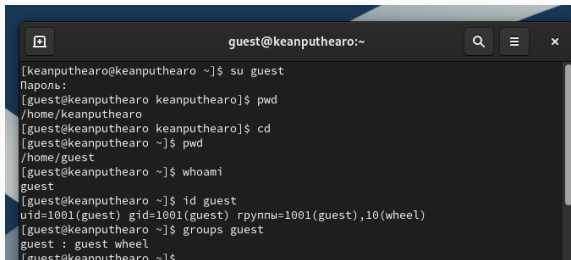
Цели и задачи работы

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

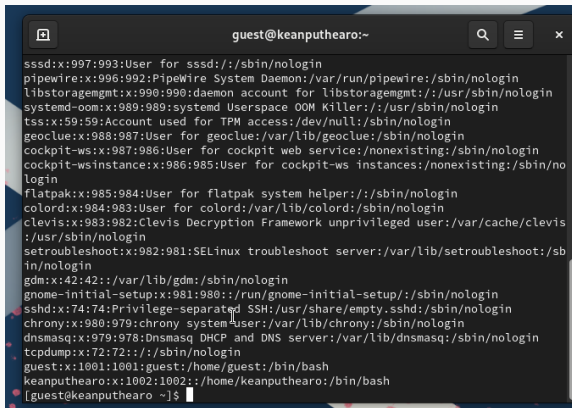
Определяем UID и группу



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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@keanputhearo:~' with search, menu, and close icons in the title bar. The terminal displays the output of the 'cat /etc/passwd' command, listing system and regular users. The output is as follows:

```
sssd:x:997:993:User for sssd:/usr/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/usr/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:/usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/usr/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexistent:/usr/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexistent:/usr/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/usr/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/usr/sbin/nologin
clevis:x:983:982:CLEVIS Decryption Framework unprivileged user:/var/cache/levis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/usr/sbin/nologin
gnome-initial-setup:x:981:980:/:/run/gnome-initial-setup:/usr/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/usr/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:/usr/sbin/nologin
guest:x:1001:1001:guest:/home/guest:/bin/bash
keanputhearo:x:1002:1002:/:/home/keanputhearo:/bin/bash
[guest@keanputhearo ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@keanputhearo ~]$  
[guest@keanputhearo ~]$ ls -l /home/  
итого 8  
drwx-----, 14 guest      guest      4096 сен 12 11:28 guest  
drwx-----, 14 keanputhearo keanputhearo 4096 сен 12 11:25 keanputhearo  
[guest@keanputhearo ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@keanputhearo ~]$  
[guest@keanputhearo ~]$ cd  
[guest@keanputhearo ~]$ mkdir dir1  
[guest@keanputhearo ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 сен 12 11:37 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@keanputhearo ~]$ chmod 000 dir1  
[guest@keanputhearo ~]$ ls -l dir1/  
ls: невозможно открыть каталог 'dir1/': Отказано в доступе  
[guest@keanputhearo ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@keanputhearo ~]$
```

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.