

Дискреционное разграничение прав в Linux. Основные атрибуты

Исмаил Айман¹

10 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

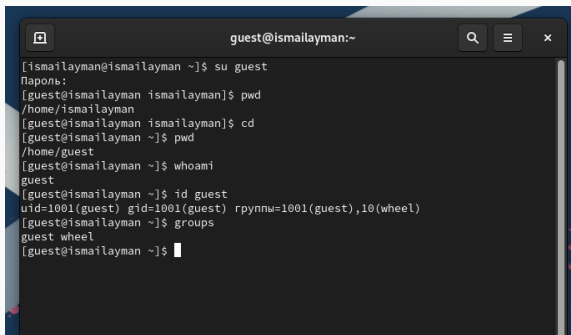
Цели и задачи работы

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

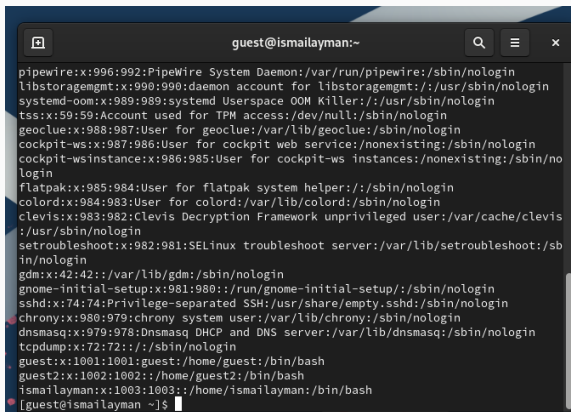
Определяем UID и группу



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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@ismailayman:~' displays the contents of the /etc/passwd file. The window has a dark background with light-colored text. The output shows a list of system and regular users, each with their username, UID, GID, and shell path. The users listed include pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, sshd, chrony, dnsmasq, tcpdump, guest, guest2, and ismailayman. The prompt '[guest@ismailayman ~]\$' is visible at the bottom.

```
guest@ismailayman:~  
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/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  
tcpdump:x:72:72:/:/sbin/nologin  
guest:x:1001:1001:guest:/home/guest:/bin/bash  
guest2:x:1002:1002:/:home/guest2:/bin/bash  
ismailayman:x:1003:1003:/:home/ismailayman:/bin/bash  
[guest@ismailayman ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@ismailayman ~]$  
[guest@ismailayman ~]$  
[guest@ismailayman ~]$ ls -l /home  
итого 8  
drwx-----. 14 guest      guest      4096 сен 10 11:07 guest  
drwx-----.  3 guest2     guest2     78 сен 17  2023 guest2  
drwx-----. 14 ismailayman ismailayman 4096 сен 10 11:03 ismailayman  
[guest@ismailayman ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@ismailayman ~]$  
[guest@ismailayman ~]$  
[guest@ismailayman ~]$ cd  
[guest@ismailayman ~]$ mkdir dir1  
[guest@ismailayman ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 сен 10 11:12 dir1  
[guest@ismailayman ~]$ echo test > dir1/file1  
[guest@ismailayman ~]$ cd dir1/  
[guest@ismailayman dir1]$ cd..  
bash: cd..: command not found..  
[guest@ismailayman dir1]$ cd ..  
[guest@ismailayman ~]$ chmod 000 dir1/  
[guest@ismailayman ~]$ ls -l | grep dir1  
d------. 2 guest guest 19 сен 10 11:13 dir1  
[guest@ismailayman ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@ismailayman ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@ismailayman ~]$
```

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.