

Дискреционное разграничение прав в Linux. Основные атрибуты

Свояк Валерия НБИ-01-20¹

10 сентября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

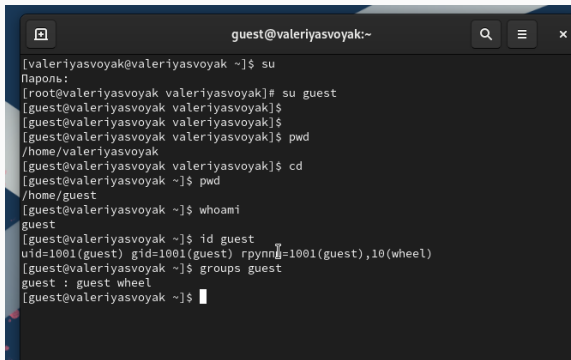
Цели и задачи работы

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

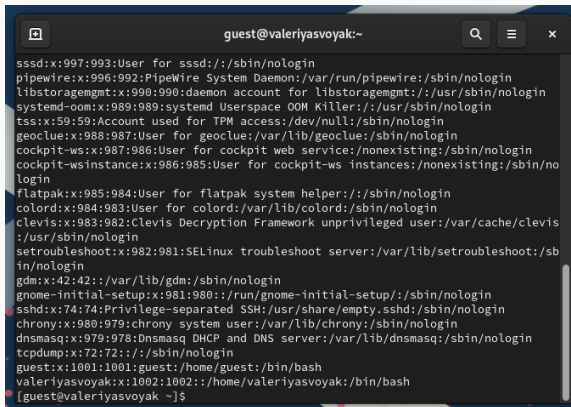
Определяем UID и группу

A terminal window titled 'guest@valeriyasvoyak:~' with search, menu, and close icons. It shows a series of commands and their outputs to determine the user's identity. The commands include 'su', 'su guest', 'pwd', 'cd', 'whoami', 'id guest', and 'groups guest'. The output of 'id guest' shows 'uid=1001(guest) gid=1001(guest) rpynd=1001(guest),10(wheel)'. The output of 'groups guest' shows 'guest : guest wheel'.

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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window with a dark background and light text. The title bar shows 'guest@valeriyasvoyak:~'. The terminal displays the output of a command that lists the contents of the /etc/passwd file. Each line represents a system or regular user, showing their username, UID, GID, and shell path. The users listed include sssd, pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, sshd, chrony, dnsmasq, tcpdump, guest, and valeriyasvoyak. The prompt at the bottom is '[guest@valeriyasvoyak ~]\$'.

```
guest@valeriyasvoyak:~  
sssd:x:997:993: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  
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 Encryption Framework unprivileged user:/var/cache/clevis  
:/usr/sbin/nologin  
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sb  
in/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  
valeriyasvoyak:x:1002:1002:/:home/valeriyasvoyak:/bin/bash  
[guest@valeriyasvoyak ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@valeriyasvoyak ~]$  
[guest@valeriyasvoyak ~]$ ls -l /home/  
итого 8  
drwx-----. 14 guest          guest          4096 сен 10 14:33 guest  
drwx-----. 14 valeriyasvoyak valeriyasvoyak 4096 сен 10 14:44 valeriyasvoyak  
[guest@valeriyasvoyak ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@valeriyasvoyak ~]$  
[guest@valeriyasvoyak ~]$ cd  
[guest@valeriyasvoyak ~]$ mkdir dir1  
[guest@valeriyasvoyak ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 сен 10 14:51 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@valeriyasvoyak ~]$ chmod 000 dir1  
[guest@valeriyasvoyak ~]$ ls -l dir1/  
ls: невозможно открыть каталог 'dir1/': Отказано в доступе  
[guest@valeriyasvoyak ~]$ echo "test" > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@valeriyasvoyak ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@valeriyasvoyak ~]$
```

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.