

Дискреционное разграничение прав в Linux. Основные атрибуты

Никита Надежда¹

7 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

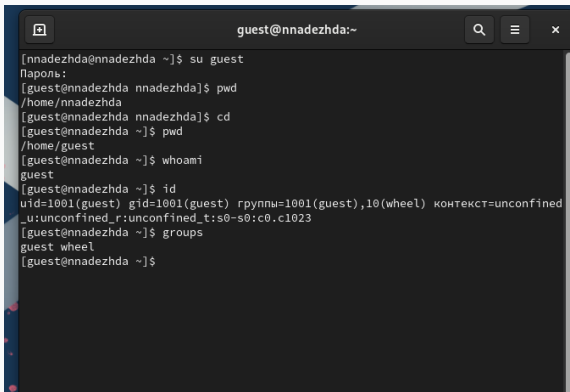
Цели и задачи работы

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

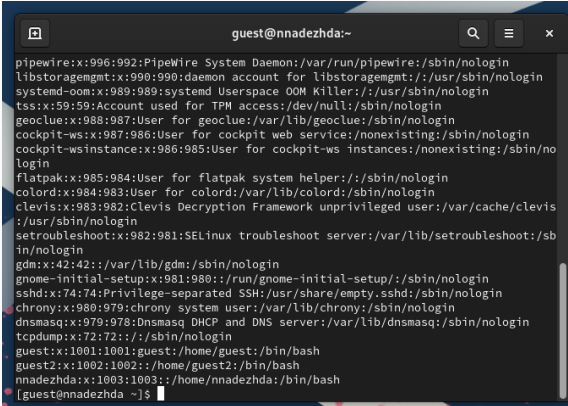
Определяем UID и группу

A terminal window titled 'guest@nnadezhda:~' with search, menu, and close icons in the title bar. The terminal shows a sequence of commands and their outputs: switching to the 'guest' user, checking the password, the current directory, the current directory again, and finally running 'whoami' and 'id'. The 'id' command output shows the user is 'guest' with UID 1001, GID 1001, and is a member of the 'wheel' group. The 'groups' command confirms the 'wheel' group membership.

```
guest@nnadezhda:~  
[nnadezhda@nnadezhda ~]$ su guest  
Пароль:  
[guest@nnadezhda nnadezhda]$ pwd  
/home/nnadezhda  
[guest@nnadezhda nnadezhda]$ cd  
[guest@nnadezhda ~]$ pwd  
/home/guest  
[guest@nnadezhda ~]$ whoami  
guest  
[guest@nnadezhda ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined  
_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@nnadezhda ~]$ groups  
guest wheel  
[guest@nnadezhda ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@nnadezhda:~' with search, menu, and close icons in the title bar. The terminal displays the output of the 'cat /etc/passwd' command, showing a list of system and regular users. Each line represents a user entry in the format 'username:x:UID:GID:full_name:home_directory:shell'.

```
guest@nnadezhda:~  
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:/usr/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:GDM User:/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:981:980:GNOME Initial Setup:/usr/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:guest2:/home/guest2:/bin/bash  
nnadezhda:x:1003:1003:nnadezhda:/home/nnadezhda:/bin/bash  
[guest@nnadezhda ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@nnadezhda ~]$  
[guest@nnadezhda ~]$  
[guest@nnadezhda ~]$ ls -l /home  
иторо 8  
drwx-----, 14 guest      guest      4096 сен  7 15:40 guest  
drwx-----,  3 guest2     guest2     78 сен 17 2023 guest2  
drwx-----, 14 nnadezhda  nnadezhda 4096 сен  7 15:38 nnadezhda  
[guest@nnadezhda ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@nnadezhda ~]$ cd
[guest@nnadezhda ~]$ mkdir dir1
[guest@nnadezhda ~]$ ls -l | grep dir1
drwxr-xr-x. 2 guest guest 6 сен  7 15:45 dir1
[guest@nnadezhda ~]$ chmod 000 dir1
[guest@nnadezhda ~]$ ls -l | grep dir1
d----- . 2 guest guest 6 сен  7 15:45 dir1
[guest@nnadezhda ~]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@nnadezhda ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@nnadezhda ~]$
```

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.