

Дискреционное разграничение прав в Linux. Основные атрибуты

Егор Судаков НБИ-01-20¹

12 сентября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

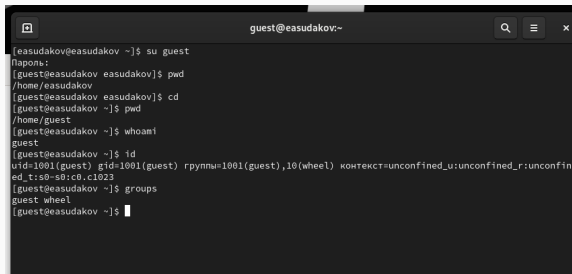
Цели и задачи работы

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

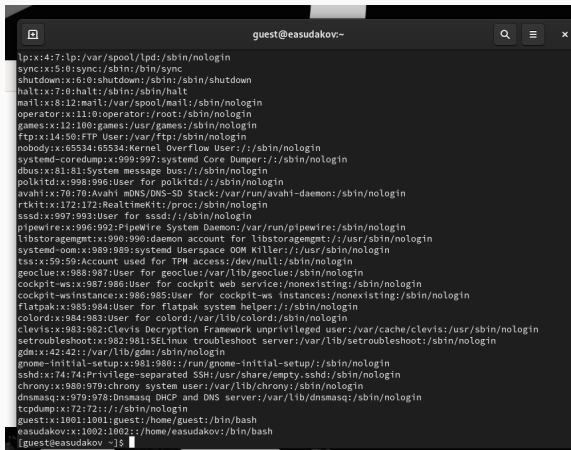
Определяем UID и группу

A terminal window titled 'guest@easudakov:~' with search, menu, and close icons in the title bar. The terminal shows a sequence of commands and their outputs: 'su guest' switches to the 'guest' user; 'pwd' shows the current directory as '/home/easudakov'; 'cd' changes to the user's home directory; 'whoami' confirms the user is 'guest'; 'id' displays the user's identity, including UID=1001, GID=1001, and the 'wheel' group; 'groups' lists the 'wheel' group.

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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@easudakov:~' displays the contents of the /etc/passwd file. The output is a list of system and user accounts, each on a new line, showing their username, UID, GID, and shell path. The window has a dark theme and standard terminal icons in the title bar.

```
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:999:990: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:/nonexistent:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexistent:/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
easudakov:x:1002:1002:/home/easudakov:/bin/bash
[guest@easudakov ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
easudakov:x:1002:1002:~/home/easudakov:/bin/bash
[guest@easudakov ~]$
[guest@easudakov ~]$ ls -l /home
итого 8
drwx-----. 14 easudakov easudakov 4096 сен 12 19:36 easudakov
drwx-----. 14 guest      guest      4096 сен 12 19:39 guest
[guest@easudakov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@easudakov ~]$  
[guest@easudakov ~]$ cd  
[guest@easudakov ~]$ mkdir dir1  
[guest@easudakov ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 сен 12 19:46 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@easudakov ~]$ chmod 000 dir1  
[guest@easudakov ~]$ ls -l dir1/  
ls: невозможно открыть каталог 'dir1/': Отказано в доступе  
[guest@easudakov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@easudakov ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@easudakov ~]$
```

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.