

Дискреционное разграничение прав в Linux. Основные атрибуты

Саинт-Амур Измаэль Нпибд-02-20¹

11 сентября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

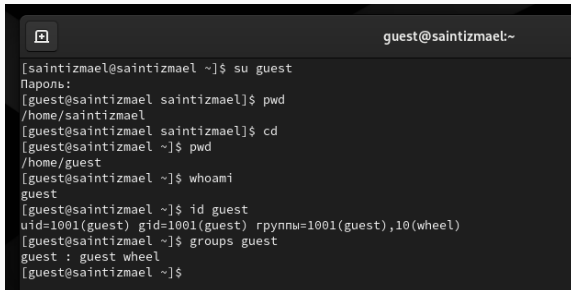
Цели и задачи работы

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

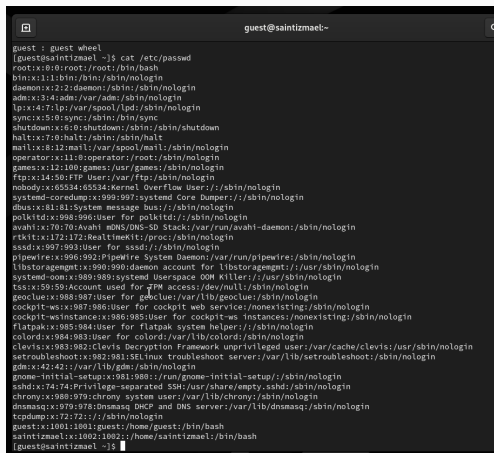
Определяем UID и группу



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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window with the title 'guest@saintizmael~' shows the command 'cat /etc/passwd' being executed. The output lists system and regular users in a standard passwd file format, including fields for username, UID, GID, name, home directory, and shell. The users listed are: daemon, adm, lp, sync, shutdown, halt, mail, operator, games, ftp, nobody, systemd-coredump, dbus, polkitd, avahi, rtkit, sssd, pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, ssshd, chrony, dnsmasq, and tpcdump, followed by the regular users 'guest' and 'saintizmael'.

```
guest : guest wheel
[guest@saintizmael ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
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: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
tpcdump:x:72:72:/:/sbin/nologin
guest:x:1001:1001:guest:/home/guest:/bin/bash
saintizmael:x:1002:1002:/home/saintizmael:/bin/bash
[guest@saintizmael ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@saintizmael ~]$  
[guest@saintizmael ~]$ ls -l /home/  
итого 8  
drwx-----, 14 guest      guest      4096 сен 11 17:26 guest  
drwx-----, 14 saintizmael saintizmael 4096 сен 11 17:24 saintizmael  
[guest@saintizmael ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@saintizmael ~]$ cd
[guest@saintizmael ~]$ mkdir dir1
[guest@saintizmael ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 11 17:33 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@saintizmael ~]$ chmod 000 dir1/
[guest@saintizmael ~]$ ls -l dir1/
ls: невозможно открыть каталог 'dir1/': Отказано в доступе
[guest@saintizmael ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@saintizmael ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@saintizmael ~]$
```

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.