

Дискреционное разграничение прав в Linux. Основные атрибуты

Дессие Абди Бедаса¹

10 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

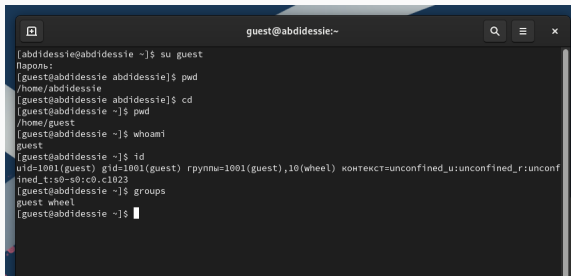
Цели и задачи работы

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

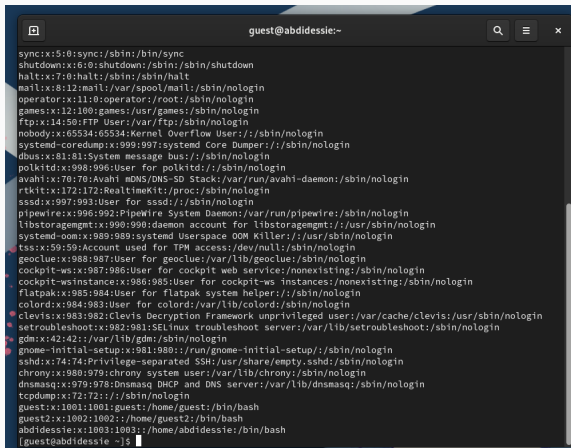
Определяем UID и группу

A terminal window titled 'guest@abdidessie:~' with search, menu, and close icons. It shows a sequence of commands to switch to the 'guest' user and retrieve system information. The output of 'id' shows the user is 'guest' with UID 1001 and GID 1001, belonging to the 'wheel' group. The output of 'groups' shows the user belongs to the 'wheel' group.

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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A screenshot of a terminal window with a dark background. The title bar shows 'guest@abdiessie:~'. The terminal displays the output of a command, listing system and user accounts in a colon-separated format. The entries include system users like 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, and gnome-initial-setup, followed by regular users guest, guest2, abdiessie, and the current user guest. The prompt '[guest@abdiessie ~]\$' is visible at the bottom.

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

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
guest:x:1001:1001:guest:/home/guest:/bin/bash
guest2:x:1002:1002::/home/guest2:/bin/bash
abdidessie:x:1003:1003::/home/abdidessie:/bin/bash
[guest@abdidessie ~]$
[guest@abdidessie ~]$
[guest@abdidessie ~]$ ls -l /home
итого 8
drwx-----, 14 abdidessie abdidessie 4096 сен 10 11:26 abdidessie
drwx-----, 14 guest      guest      4096 сен 10 11:27 guest
drwx-----,  3 guest2     guest2     78 сен 17 2023 guest2
[guest@abdidessie ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@abdidessie ~]$  
[guest@abdidessie ~]$ cd  
[guest@abdidessie ~]$ mkdir dir1  
[guest@abdidessie ~]$ ls -l | grep dir1/  
[guest@abdidessie ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 сен 10 11:35 dir1  
[guest@abdidessie ~]$ chmod 000 dir1/  
[guest@abdidessie ~]$ ls -l | grep dir1  
d------. 2 guest guest 6 сен 10 11:35 dir1  
[guest@abdidessie ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@abdidessie ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@abdidessie ~]$
```

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.