

Дискреционное разграничение прав в Linux. Основные атрибуты

Еде Мак Дональд Чуквума ¹

12 сентября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

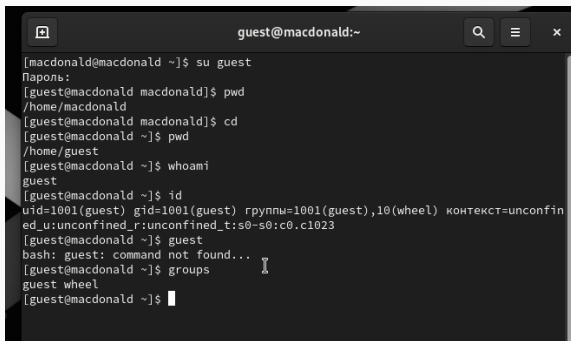
Цели и задачи работы

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

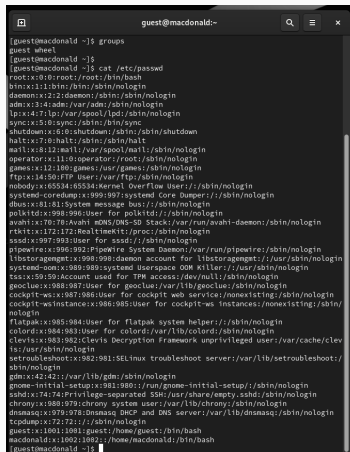
Определяем UID и группу



```
guest@macdonald:~  
[macdonald@macdonald ~]$ su guest  
Пароль:  
[guest@macdonald macdonald]$ pwd  
/home/macdonald  
[guest@macdonald macdonald]$ cd  
[guest@macdonald ~]$ pwd  
/home/guest  
[guest@macdonald ~]$ whoami  
guest  
[guest@macdonald ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@macdonald ~]$ guest  
bash: guest: command not found...  
[guest@macdonald ~]$ groups  
guest wheel  
[guest@macdonald ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@macdonald:~' with search, menu, and close icons in the title bar. The terminal shows the command '[guest@macdonald ~]\$ cat /etc/passwd' and its output, which lists system and regular users with their IDs, home directories, and shells. The output is as follows:

```
[guest@macdonald ~]$ cat /etc/passwd
guest:x:0:0:root:/root:/bin/bash
daemon: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-D Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:992:User for sssd:/:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragenet:x:998:998:daemon account for libstoragenet:/:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:/usr/sbin/nologin
tss:x:50:50:Account used for TPM access:/dev/null:/sbin/nologin
goclue:x:988:987:User for goclue:/var/lib/goclue:/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
macdonald:x:1002:1002:/home/macdonald:/bin/bash
[guest@macdonald ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@macdonald ~]$  
[guest@macdonald ~]$ ls -l /home/  
итого 8  
drwx-----, 14 guest      guest      4096 сен 12 20:01 guest  
drwx-----, 14 macdonald  macdonald 4096 сен 12 19:59 macdonald  
[guest@macdonald ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@macdonald ~]$  
[guest@macdonald ~]$ ls -l /home/  
итого 8  
drwx-----, 14 guest      guest      4096 сен 12 20:01 guest  
drwx-----, 14 macdonald  macdonald 4096 сен 12 19:59 macdonald  
[guest@macdonald ~]$  
[guest@macdonald ~]$  
[guest@macdonald ~]$ cd  
[guest@macdonald ~]$ mkdir dir1  
[guest@macdonald ~]$ ls -l  
итого 0  
drwxr-xr-x, 2 guest guest 6 сен 12 20:08 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@macdonald ~]$ chmod 000 dir1/  
[guest@macdonald ~]$ ls -l  
итого 0  
d-----, 2 guest guest 6 сен 12 20:08 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@macdonald ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@macdonald ~]$
```

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.