

Дискреционное разграничение прав в Linux. Основные атрибуты

Герра Гарсия Паола Валентина¹

22 февраля, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

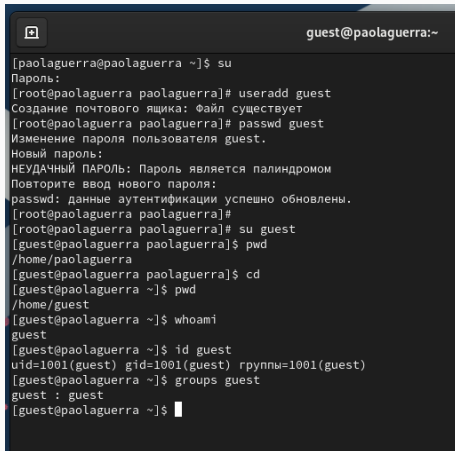
Цели и задачи работы

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

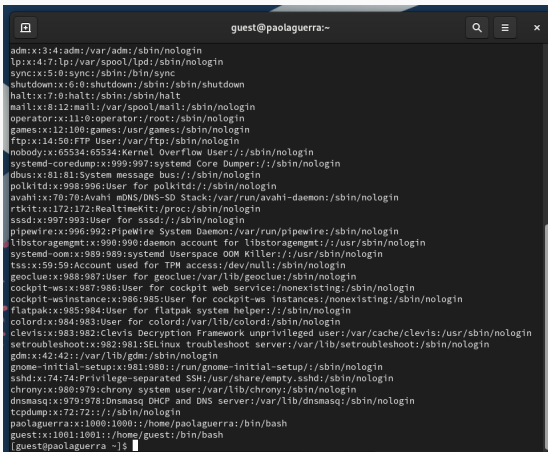
Определяем UID и группу



```
guest@paolaguerra:~  
[paolaguerra@paolaguerra ~]$ su  
Пароль:  
[root@paolaguerra paolaguerra]# useradd guest  
Создание почтового ящика: Файл существует  
[root@paolaguerra paolaguerra]# passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[root@paolaguerra paolaguerra]#  
[root@paolaguerra paolaguerra]# su guest  
[guest@paolaguerra paolaguerra]$ pwd  
/home/paolaguerra  
[guest@paolaguerra paolaguerra]$ cd  
[guest@paolaguerra ~]$ pwd  
/home/guest  
[guest@paolaguerra ~]$ whoami  
guest  
[guest@paolaguerra ~]$ id guest  
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest)  
[guest@paolaguerra ~]$ groups guest  
guest : guest  
[guest@paolaguerra ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@paolaguerra:~' displays the contents of the /etc/passwd file. The window has a dark background and standard terminal window controls (minimize, maximize, close) in the top right corner. The output is a list of system and user accounts, each on a new line, showing their username, UID, GID, and shell path. The list includes system users like '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', 'cockpit-ws-instance', 'flatpak', 'colord', 'clevis', 'setroubleshoot', 'gdm', 'gnome-initial-setup', 'ssh', 'chrony', 'dnsmasq', and 'tcpdump', followed by regular users 'paolaguerra' and 'guest'.

```
guest@paolaguerra:~  
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-ws-instance: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  
ssh: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  
paolaguerra:x:1000:1000:/home/paolaguerra:/bin/bash  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@paolaguerra ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@paolaguerra ~]$  
[guest@paolaguerra ~]$ ls -l /home/  
итого 4  
drwx-----, 3 guest      guest      78 фев 22 15:40 guest  
drwx-----, 14 paolaguerra paolaguerra 4096 фев 22 15:38 paolaguerra  
[guest@paolaguerra ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@paolaguerra ~]$  
[guest@paolaguerra ~]$ cd  
[guest@paolaguerra ~]$ mkdir dir1  
[guest@paolaguerra ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 фев 22 15:46 dir1  
[guest@paolaguerra ~]$ chmod 000 dir1/  
[guest@paolaguerra ~]$ ls -l  
итого 0  
d------. 2 guest guest 6 фев 22 15:46 dir1  
[guest@paolaguerra ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@paolaguerra ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@paolaguerra ~]$
```

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.