

Дискреционное разграничение прав в Linux. Основные атрибуты

Герра Гарсия Максимиано Антонио¹

22 февраля, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

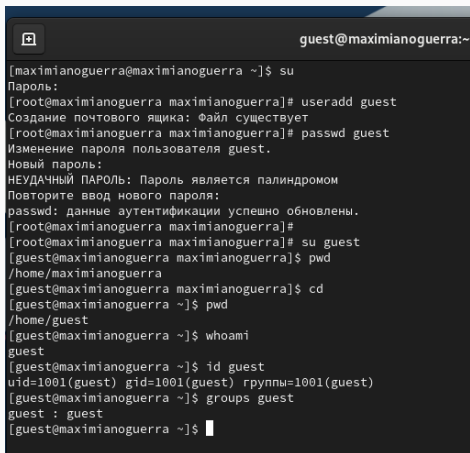
Цели и задачи работы

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

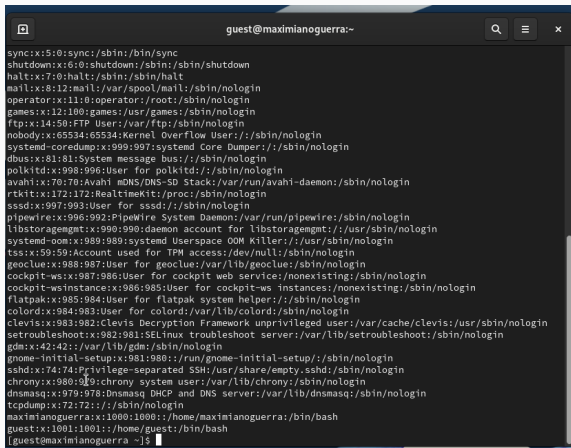
Определяем UID и группу



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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window with a dark background and light text. The title bar shows 'guest@maximianoguerra:~'. The terminal displays the output of a command that lists the contents of the /etc/passwd file. Each line represents a system or regular user, showing their username, UID, GID, and home directory/shell path. The users listed include sync, shutdown, halt, mail, operator, games, ftp, nobody, systemd-coredump, dbus, polkitd, avahi, rtkit, sssd, pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, sshd, chrony, dnsmasq, and tcpdump. The prompt at the bottom is '[guest@maximianoguerra ~]\$' with a cursor.

```
guest@maximianoguerra:~
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
maximianoguerra:x:1000:1000:/home/maximianoguerra:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@maximianoguerra ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@maximianoguerra ~]$  
[guest@maximianoguerra ~]$  
[guest@maximianoguerra ~]$ ls -l /home  
иторо 4  
drwx-----, 3 guest          guest          78 фев 22 15:16 guest  
drwx-----, 14 maximianoguerra maximianoguerra 4096 фев 22 15:15 maximianoguerra  
[guest@maximianoguerra ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

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

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.