

Дискреционное разграничение прав в Linux. Основные атрибуты

Еюбоглу Тимур¹

23 февраля, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

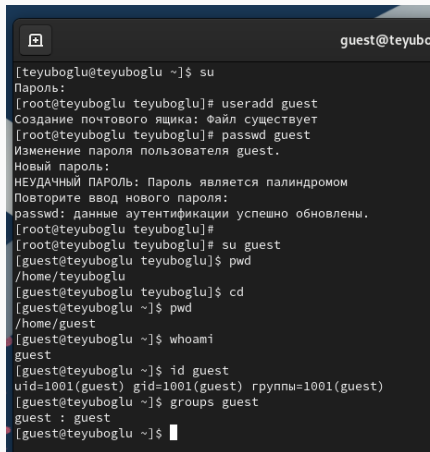
Цели и задачи работы

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

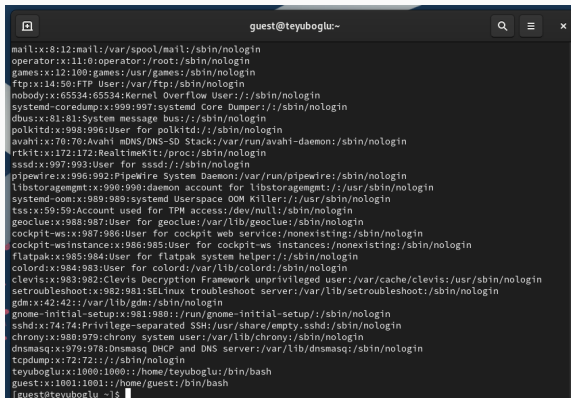


```
guest@teyubo

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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



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

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
dnsmasq:x:919:918:dnsmasq:dnsmasq and dns server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
teyuboglu:x:1000:1000::/home/teyuboglu:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@teyuboglu ~]$
[guest@teyuboglu ~]$
[guest@teyuboglu ~]$ ls -l /home
итого 4
drwx-----. 3 guest      guest      78 фев 23 14:06 guest
drwx-----. 14 teyuboglu teyuboglu 4096 фев 23 14:02 teyuboglu
[guest@teyuboglu ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@teyuboglu ~]$  
[guest@teyuboglu ~]$ cd  
[guest@teyuboglu ~]$ mkdir dir1  
[guest@teyuboglu ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 фев 23 14:11 dir1  
[guest@teyuboglu ~]$ chmod 000 dir1  
[guest@teyuboglu ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 фев 23 14:11 dir1  
[guest@teyuboglu ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@teyuboglu ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@teyuboglu ~]$
```

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.