Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Ким Реачна[1]

15 сентября, 2023, Москва, Россия

[1]Российский Университет Дружбы Народов

Вводная часть

Цели и задачи

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Процесс выполнения лабораторной работы

Определяем UID и группу

```
[kreachna@kreachna ~]$ su guest
Password:
[guest@kreachna kreachna]$ pwd
/home/kreachna
[guest@kreachna kreachna]$ cd
[guest@kreachna ~]$ pwd
/home/guest
[guest@kreachna ~]$ whoami
guest
[guest@kreachna ~]$ id guest
uid=1001(guest) gid=1001(guest) groups=1001(guest)
[guest@kreachna ~]$ groups guest
guest : guest
```

Рис. 1: Информация о пользователе guest

Файл с данными о пользователях

```
[guest@kreachna ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin: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-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
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
kreachna:x:1000:1000:kreachna:/home/kreachna:/bin/bash
vboxadd:x:977:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@kreachna ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
```

Рис. 2: Сожержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@kreachna ~]$ ls -l /home/
total 4
drwx------.  4 guest    guest     112 Sep 16 12:00 guest
drwx------. 14 kreachna kreachna 4096 Sep 16 11:40 kreachna
[guest@kreachna ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/kreachna
---------------------- /home/guest
```

Рис. 3: Расширенные атрибуты

Атрибуты директории

```
[guest@kreachna ~]$ chmod 000 dir1
[guest@kreachna ~]$ ls -l
total 0
d---------. 2 guest guest 6 Sep 16 12:11 dir1
[guest@kreachna ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@kreachna ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@kreachna ~]$
```

Рис. 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)

Рис. 5: Минимальные права для совершения операций

Выводы по проделанной работе

Вывод

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.