Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ильин А.В.

7 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ильин Андрей Владимирович
- НФИбд-01-20
- 1032201656
- Российский Университет Дружбы Народов
- 1032201656@pfur.ru
- https://github.com/av-ilin

Вводная часть

Актуальность

- Приобрести необхдимые в современном научном сообществе навыки администрирования систем и информационной безопасности.

Цель

- Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Задачи

1. Создать программу способную выводить gid, uid и провести исследование SetUID-битов.
2. Исследовать Sticky-бит.

Материалы и методы

- Rocky Linux
- Git
- VirtualBox

Выполнение работы

simpleid.c и simpleid2.c

Рис. 1: Запуск simpleid.c и simpleid2.c

`simpleid2.c` с измененным владельцем и аттрибутами

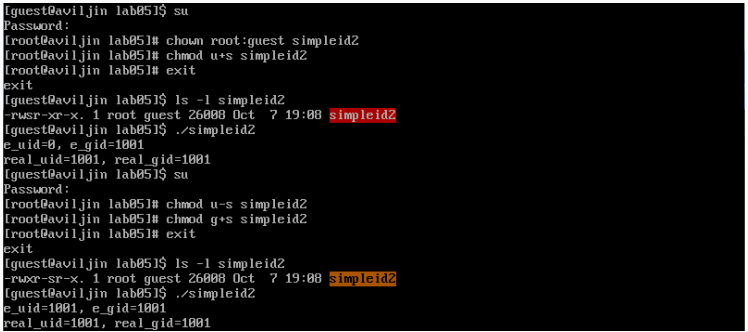

Рис. 2: Запуск `simpleid2.c` с измененным владельцем и аттрибутами

Подготовка к запуску `readfile`

Рис. 3: Подготовка к запуску `readfile`

Запуск `readfile`

```
[guest@aviljin lab05]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

int main (int argc, char* argv[]) {
    unsigned char buffer[16];
    size_t bytes_read;
    int i;
    int fd = open (argv[1], O_RDONLY);

    do {
        bytes_read = read(fd, buffer, sizeof (buffer));
        for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]);
    }

    while (bytes_read == sizeof (buffer));
    close(fd);
    return 0;
}[guest@aviljin lab05]$ S
```

Рис. 4: Запуск `readfile` (`readfile.c`)

```
[guest@aviljin lab05]$ ./readfile /etc/shadow
root:$6$tyv.S/YLIKlGzpUF$nbzG39i9.GSkS1Q9h13GumO8dVhAnxzWRM7S96J4uudObBt4PfKflcB9i0BKGPD43sb.PtuHMJ6
/AGexSNx.c0::0:99999:7:::
bin:*:19469:0:99999:7:::
daemon:*:19469:0:99999:7:::
adm:*:19469:0:99999:7:::
lp:*:19469:0:99999:7:::
sync:*:19469:0:99999:7:::
shutdown:*:19469:0:99999:7:::
halt:*:19469:0:99999:7:::
mail:*:19469:0:99999:7:::
operator:*:19469:0:99999:7:::
games:*:19469:0:99999:7:::
ftp:*:19469:0:99999:7:::
nobody:*:19469:0:99999:7:::
systemd-coredump:!!:19608::::::
dbus:!!:19608::::::
tss:!!:19608::::::
sssd:!!:19608::::::
sshd:!!:19608::::::
chrony:!!:19608::::::
systemd-oom:!*:19608::::::
aviljin:$6$4sCrU02PIw4pEDa$8.jeQaFthE6.jRBkgmWohs/wQiIMqP.5e0AEaeMbfGIRp.0aE2Yu91Rb0BShmgKVtjQKkSrIP2
sEJ1.7rifwAA0:19608:0:99999:7:::
guest:$6$CisIYOy0G5Y1tmqa$FQs3U6rwjabThOhqdGLqXiW9Fgt2T.hMpXDcCAHBp1IwlIFMBXqBCbHq4SM4nk5mKTsWSFN3fc
K/zuUh5CKOo/:19616:0:99999:7:::
guest2:$6$29q46ZDN3X4NxqvU$M2efihsg0my3bC4z5oGUqumo5oQyHZJ2.pySsbh8G1h8M2rtkFwAJVljtAH39/XfKtwImKCnQs
SHKFnA0pJMB18:19623:0:99999:7:::
```

Рис. 5: Запуск `readfile` (`/etc/shadow`)

Подготовка к исследованию Sticky-бита

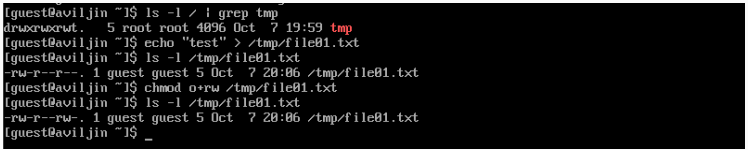

Рис. 6: Атрибут Sticky

Исследование Sticky-бита

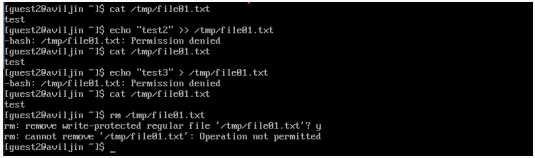

Рис. 7: Исследование Sticky (1)

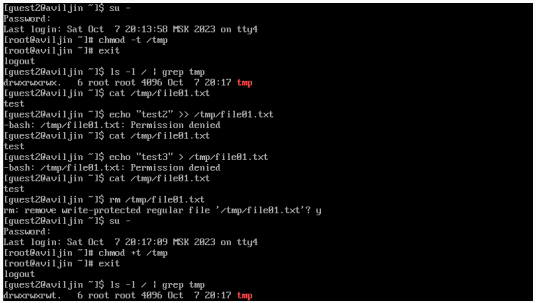

Рис. 8: Исследование Sticky (2)

Результаты

Итог

- Изучены идентификаторы SetUID-биты и Sticky-биты. Опробовали их действие на практике. Изучили влияние бита Sticky. Повысили свои навыки использования интерфейса командой строки (CLI).

Спасибо за внимание!