Лабораторная работа №5

Информационная безопасность

Николаев Д. И.

3 октября 2023

Российский университет дружбы народов, Москва, Россия

Прагматика выполнения

Прагматика выполнения

- Повышение навыков использования интерфейса командой строки (CLI);
- Знакомство с атрибутами SetUID-, SetGID- и Stycky-битов;
- Применение полученных знаний на практике в дальнейшем.

Цели

Цели

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

Задачи

1. Закрепить основы дискреционного разграничения доступа;
2. Проверить работу атрибутов SetUID-, SetGID- и Stycky-битов.

Выполнение работы

Установка SetUID-бита

SetUID разрешает пользователям запускать исполняемые файлы с правами владельца исполняемого файла.

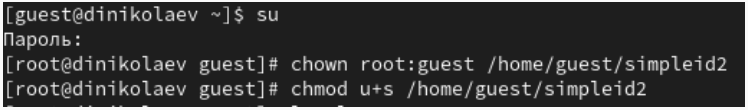

Рис. 1: Изменение владельца и прав доступа к файлу simpleid2

Результат установки SetUID-бита 1

```
[guest@dinikolaev ~]$ ./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;
}
```

Рис. 2: Чтение программы readfile.c с помощью readfile

Результат установки SetUID-бита 2

```
[guest@dinikolaev ~]$ ./readfile /etc/shadow
root:$6$uzIWDVIM3DxZGIjE$9qg5cxA6EOTfuNBIIgx2Z0//pL88Kd9wyiGtIFzRrpFV6mzYk7gvNvn
Ysr71YYz64WuASk0wdSMlWw3X133Fx1::0:99999:7:::
bin:*:19347:0:99999:7:::
daemon:*:19347:0:99999:7:::
adm:*:19347:0:99999:7:::
lp:*:19347:0:99999:7:::
sync:*:19347:0:99999:7:::
shutdown:*:19347:0:99999:7:::
halt:*:19347:0:99999:7:::
mail:*:19347:0:99999:7:::
operator:*:19347:0:99999:7:::
games:*:19347:0:99999:7:::
ftp:*:19347:0:99999:7:::
nobody:*:19347:0:99999:7:::
systemd-coredump:!!:19609::::::
dbus:!!:19609::::::
polkitd:!!:19609::::::
avahi:!!:19609::::::
rtkit:!!:19609::::::
libstoragemgmt:*:19609::::::
systemd-oom:!*:19609::::::
geoclue:!!:19609::::::
tss:!!:19609::::::
cockpit-ws:!!:19609::::::
cockpit-wsinstance:!!:19609::::::
colord:!!:19609::::::
sssd:!!:19609::::::
setroubleshoot:!!:19609::::::
pipewire:!!:19609::::::
flatpak:!!:19609::::::
clevis:!!:19609::::::
gdm:!!:19609::::::
gnome-initial-setup:!!:19609::::::
pesign:!!:19609::::::
sshd:!!:19609::::::
chrony:!!:19609::::::
dnsmasq:!!:19609::::::
tcpdump:!!:19609::::::
dinikolaev:$6$0G3AyU5kR.xSl1jM$M2E7uM4922DFie0dxezgNytTvaK6tvwGKOJieU6XiTVo40HPA
i/CojkdE4j0Qo0ZswzQb8cnS2IHu9mDSSFCw1::0:99999:7:::
vboxadd:!!:19609::::::
guest:$6$etabJ3/NOQ3ix/OV$H01ObUdzNJ14goI7Kw.RN.KQXXft2x7AtaynDbv33XA2.tnf3jPnEi
ezg2f2DJwGCl8lNZTtt1csS339fZYqt0:19613:0:99999:7:::
guest2:$6$Wxw4hbXdWkXoFwta$24cbNSXNtNRSkEegqlf8vhNcNh0hzoOP/XhO6SfY52WR4OUNIo0PV
mUQKwnccBP6F5Oo9FHfNwx7joom6Xvm5.:19623:0:99999:7:::
```

В случае, если этот бит установлен для папки, то файлы в этой папке могут быть удалены только их владельцем.

```
[guest@dinikolaev ~]$ ls -l / | grep tmp
drwxrwxrwt.  17 root root 4096 окт  3 15:57 tmp
[guest@dinikolaev ~]$ echo "test" > /tmp/file01.txt
[guest@dinikolaev ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 окт  3 16:02 /tmp/file01.txt
[guest@dinikolaev ~]$ chmod o+rw /tmp/file01.txt
[guest@dinikolaev ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 окт  3 16:02 /tmp/file01.txt
[guest@dinikolaev ~]$
```

Рис. 4: Проверка Sticky-бита и создание файла file01.txt с правами на чтение и запись

Результат применения Sticky-бита

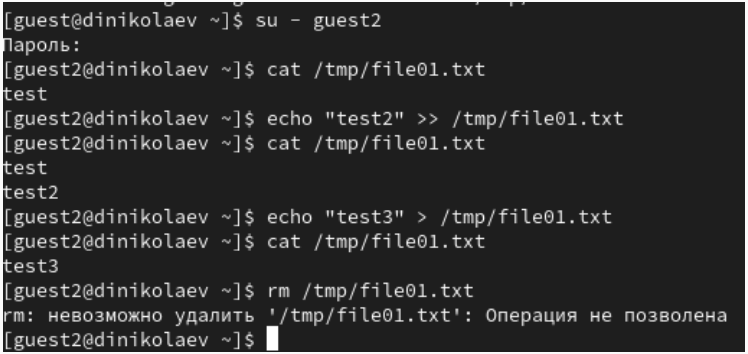

Рис. 5: Проверка некоторых действий с файлом file01.txt от имени пользователя guest2

Результат при отсутствии Sticky-бита

Рис. 6: Проверка некоторых действий с файлом file01.txt без Sticky-бита от имени пользователя guest2

Результаты

Результаты

По результатам работы, я изучил механизмы изменения идентификаторов, применения SetUID и Sticky-битов. Я получила практические навыки работы в консоли с дополнительными атрибутами. Я рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.