Презентация по лабораторной работе №5

Информационная безопасность

Чекалова Л. Р.

5 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Чекалова Лилия Руслановна
- студент 4 курса группы НФИбд-02-20
- ст. б. 1032201654
- Российский университет дружбы народов
- 1032201654@pfur.ru

Вводная часть

Актуальность

- Обеспечение безопасности

Цели и задачи

- Приобретение практических навыков работы в консоли с дополнительными атрибутами файлов
- Изучение механизмов смены идентификатора процессов пользователей
- Изучение SetUID-, SetGID- и Sticky-битов

Материалы и методы

- Веб-сервис `GitHub` для работы с репозиториями
- Программа для виртуализации ОС `VirtualBox`
- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
  - `pdf`
  - `docx`
- Автоматизация процесса создания: `Makefile`

Ход работы

Написание программы 1

```c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main()
{
    uid_t uid = geteuid();
    gid_t gid = getegid();
    printf("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Запуск программы 1

```
[guest@lrchekalova ~]$ ./simpleid
uid=1001, gid=1001
[guest@lrchekalova ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@lrchekalova ~]$
```

Модификация программы

```c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main()
{
    uid_t real_uid = getuid();
    uid_t e_uid = geteuid();

    gid_t real_gid = getgid();
    gid_t e_gid = getegid();
    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
    return 0;
}
```

Запуск модифицированной программы

```
[guest@lrchekalova ~]$ gcc simpleid2.c -o simpleid2
[guest@lrchekalova ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@lrchekalova ~]$
```

Изменение владельца файла

```
[guest@lrchekalova ~]$ su -
Пароль:
[root@lrchekalova ~]# chown root:guest /home/guest/simpleid2
[root@lrchekalova ~]# chmod u+s /home/guest/simpleid2
[root@lrchekalova ~]# ls -l simpleid2
ls: невозможно получить доступ к 'simpleid2': Нет такого файла или каталога
[root@lrchekalova ~]# ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 26064 окт  5 11:43 /home/guest/simpleid2
[root@lrchekalova ~]# ./simpleid2
-bash: ./simpleid2: Нет такого файла или каталога
[root@lrchekalova ~]# cd /home/guest
[root@lrchekalova guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@lrchekalova guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@lrchekalova guest]#
```

Написание программы 3

```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;
}
```

Изменение прав доступа

```
[root@lrchekalova guest]# chown root:root readfile.c
[root@lrchekalova guest]# chmod u+s readfile.c
[root@lrchekalova guest]# ls -l readfile.c
-rwSr--r--. 1 root root 456 окт  5 12:05 readfile.c
```

```
[root@lrchekalova ~]# chmod o-r /home/guest/readfile.c
[root@lrchekalova ~]# exit
выход
[guest@lrchekalova ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@lrchekalova ~]$
```

Проверка наличия Sticky-бита

```
[guest@lrchekalova ~]$ ls -l / | grep tmp
drwxrwxrwt.  17 root root 4096 окт  5 12:29 tmp
[guest@lrchekalova ~]$ echo "test" > /tmp/file01.txt
[guest@lrchekalova ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 окт  5 12:30 /tmp/file01.txt
[guest@lrchekalova ~]$ chmod o+rw /tmp/file01.txt
[guest@lrchekalova ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 окт  5 12:30 /tmp/file01.txt
[guest@lrchekalova ~]$
```

Попытка чтения, изменения и удаления файла

```
[guest@lrchekalova ~]$ su guest2
Пароль:
[guest2@lrchekalova guest]$ cat /tmp/file01.txt
test
[guest2@lrchekalova guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@lrchekalova guest]$
```

```
[guest2@lrchekalova guest]$ rm /tmp/file01.txt
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'? y
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@lrchekalova guest]$
```

Снятие Sticky-бита

```
[guest2@lrchekalova guest]$ su -
Пароль:
[root@lrchekalova ~]# chmod -t /tmp
[root@lrchekalova ~]# exit
выход
[guest2@lrchekalova guest]$ ls -l / | grep tmp
drwxrwxrwx.  17 root root 4096 окт  5 12:34 tmp
[guest2@lrchekalova guest]$
```

Повторная попытка чтения, записи и удаления файла

```
[guest2@lrchekalova guest]$ cat /tmp/file01.txt
test
[guest2@lrchekalova guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@lrchekalova guest]$ rm /tmp/file01.txt
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'? y
[guest2@lrchekalova guest]$ ls /tmp
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-chronyd.service-eBqpWs
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-colord.service-te7O2B
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-dbus-broker.service-TNybZb
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-fwupd.service-DS9osC
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-ModemManager.service-cHwCwQ
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-power-profiles-daemon.service-njCTdm
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-rtkit-daemon.service-2HYTg0
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-switcheroo-control.service-TaUiYt
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-systemd-logind.service-2zSk8l
systemd-private-b33f02659fc546bdbc78fc7c1990a8d8-upower.service-vpDYbO
tracker-extract-3-files.1000
vboxguest-Module.symvers
```

Результаты

Результаты работы

- Получены навыки работы с дополнительными атрибутами файлов
- Отточены навыки работы с механизмами смены владельца
- Рассмотрены принципы работы SetUID-, SetGID- и Sticky-битов