

Структура научной презентации

Простейший шаблон

Карпачев Я. О.

Российский университет дружбы народов, Москва, Россия

Информация

- Карпачев Я. О.
- студент
- Российский университет дружбы народов

Вводная часть

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

Выполняем команды данные в задании.

данные которые выводит программа совпадают с данными команды id, продвинутая программа единственная выводит 27(sudo) а не 1001(guest)

```
File Actions Edit View Help
$ ls
Desktop Documents Music Public Videos
dir1 Downloads Pictures Templates
$ touch simpleid.c
$ vim simpleid.c
$ gcc simpleid.c -o simpleid
cc1: fatal error: leid.c: No such file or directory
compilation terminated.
$ ls
Desktop Documents Music Public Templates
dir1 Downloads Pictures simpleid.c Videos
$ g++ simpleid.c
$ ls
a.out dir1 Downloads Pictures simpleid.c Videos
Desktop Documents Music Public Templates
$ ./a.out
uid=1001, gid=1001
$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest),27(sudo)
$ vim simpleid.c
$ g++ ./simpleid
/usr/bin/ld: cannot find ./simpleid: No such file or directory
collect2: error: ld returned 1 exit status
$ g++ simpleid.c
$ ./a.out
uid=1001, gid=1001
real_uid=1001, real_gid=1001
$ sudo chown root:guest /home/guest/simpleid
[sudo] password for guest:
chown: cannot access '/home/guest/simpleid': No such file or directory
$ sudo chown root:guest /home/guest/simpleid.c
$ chmod u+s /home/guest/a.out
$ sudo chown root:guest /home/guest/a.out
$ ls -l a.out
-rwxrwxr-x 1 root guest 16160 Apr  7 04:14 a.out
$ ./a.out
uid=1001, gid=1001
real_uid=1001, real_gid=1001
$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest),27(sudo)
```

пишем программу readfile (simpleid3.c) и пытаемся исполнит ее с входными данными, после изменение владельца, выдается ошибка нет прав

```
$ touch simpleid3.c
$ vim simpleid3.c
$ g++ simplei3.c
cc1plus: fatal error: simplei3.c: No such file or directory
compilation terminated.
$ ls
a.out Desktop dir1 Documents Downloads Music Pictures Public simpleid3.c simpleid.c Templates Videos
$ g++ simpleid3.c
$ esudo chown root:root a.out
/bin/sh: 26: esudo: not found
$ sudo chown root:root a.out
$ sudo chmod 400 a.out
$ cat a.out
cat: a.out: Permission denied
$ sudo chown root a.out
$ sudo chmod u+s a.out
$ a.out
/bin/sh: 32: a.out: not found
$ ./a.out
/bin/sh: 33: ./a.out: Permission denied
$ ./a.out /etc/shadow
/bin/sh: 34: ./a.out: Permission denied
$
```

Рис. 2: Команды

подготавливаем файл file01.txt к тестам в одном пользователе а потом меняем пользователя на guest3

```
> File Actions Edit View Help
$ ls -l / | grep tmp
drwxrwxrwt 14 root root 340 Apr 7 04:32 tmp
$ echo "test" > /tmp/file01.txt
$ ls -l /tmp/file01.txt
-rw-rw-r-- 1 guest guest 5 Apr 7 04:34 /tmp/file01.txt
$ chmod o+rw /tmp/file01.txt
$ ls -l /tmp/file01.txt
-rw-rw-rw- 1 guest guest 5 Apr 7 04:34 /tmp/file01.txt
$ █
```

Рис. 3: Команды

со стороны guest3 все команды работают кроме удаления файла так нет прав

```
$ cat /tmp/file01.txt
test
$ echo "test2" > /tmp/file01.txt
$ cat /tmp/file01.txt
test2
$ echo "test3" >> /tmp/file01.txt
$ cat /tmp/file01.txt
test2
test3
$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
$ su -
Password:
su: Authentication failure
$ su -
Password:
su: Authentication failure
$ su chmod -t /tmp
su: invalid option -- 't'
Try 'su --help' for more information.
$ su
Password:
su: Authentication failure
$ sudo su -
[sudo] password for guest3:
guest3 is not in the sudoers file.
$
```

через садуера снимаем -t

```
(yokarpachev@vbox)-[/tmp]
$ sudo chmod -t /tmp
[sudo] password for yokarpachev:
(yokarpachev@vbox)-[/tmp]
$
```

Рис. 5: Команды

проверяю команды через guest3, все работает даже удаление файла

```
$ ls -l | grep tmp
$ echo "test" >> /tmp/file01.txt
$ cat /tmp/file01.txt
test
$ echo "test2" > /tmp/file01.txt
$ cat /tmp/file01.txt
test2
$ ls /tmp
config-err-XceTds
file01.txt
ssh-1JjFgln79nqu
systemd-private-0d2711eae0d147a9b4575deebd2902a8-apache2.service-LHAsPH
systemd-private-0d2711eae0d147a9b4575deebd2902a8-color.service-illXDd
systemd-private-0d2711eae0d147a9b4575deebd2902a8-haveged.service-06c5Lg
systemd-private-0d2711eae0d147a9b4575deebd2902a8-ModemManager.service-yAbgMK
systemd-private-0d2711eae0d147a9b4575deebd2902a8-polkit.service-eSmmNr
systemd-private-0d2711eae0d147a9b4575deebd2902a8-systemd-logind.service-oMCqZW
systemd-private-0d2711eae0d147a9b4575deebd2902a8-upower.service-zjpsTk
$ ls -l | grep /tmp
ls: cannot access '}' : No such file or directory
ls: cannot access 'grep': No such file or directory
/tmp:
total 4
-rw-r--r-- 1 guest3 guest3 0 Apr 7 05:09 config-err-XceTds
-rw-rw-r-- 1 guest3 guest3 6 Apr 7 05:11 file01.txt
drwx----- 2 guest3 guest3 60 Apr 7 05:09 ssh-1JjFgln79nqu
drwx----- 3 root root 60 Apr 7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-apache2.service-LHAsPH
drwx----- 3 root root 60 Apr 7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-color.service-illXDd
drwx----- 3 root root 60 Apr 7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-haveged.service-06c5Lg
drwx----- 3 root root 60 Apr 7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-ModemManager.service-yAbgMK
drwx----- 3 root root 60 Apr 7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-polkit.service-eSmmNr
drwx----- 3 root root 60 Apr 7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-systemd-logind.service-oMCqZW
drwx----- 3 root root 60 Apr 7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-upower.service-zjpsTk
$ rm /tmp/file01.txt
$ █
```

Я научился применять механизмы изменения идентификаторов, применять SetUID- и Sticky-битов. ции возможны при тех или иных установленных правах. Опробовал дей- ствие на практике расширенных атрибутов «a» и «i»