

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное образовательное
учреждение высшего образования “Национальный
исследовательский университет ИТМО”

**ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И
КОМПЬЮТЕРНОЙ ТЕХНИКИ**

ЛАБОРАТОРНАЯ РАБОТА №2

“Политики безопасности Linux”

по дисциплине

“Информационная безопасность”

Выполнил:

Иванов Матвей Сергеевич

группа Р34111

Преподаватель:

Маркина Татьяна Анатольевна

г. Санкт-Петербург, 2024

Ход выполнения:

1) Установите утилиту AppArmor

Напишите bash-скрипт который будет создавать файл в директории log , записывать в него что-то, читать из него и затем удалять.

Содержание скрипта test_script.sh:

```
#!/bin/bash
mkdir -p log
echo "Test file" > log/test.txt
cat log/test.txt
rm -f log/test.txt
```

2) Создайте директорию log. Выдайте файлу права на исполнение. Запустите файл, покажите вывод ./file

```
s335105@v132798:~$ chmod +x test_script.sh
s335105@v132798:~$ ./test_script.sh
Test file
s335105@v132798:~$
```

3) Создайте профиль безопасности для данной программы

```
s335105@v132798:~$ su root
Password:
root@v132798:/home/s335105# sudo aa-genprof ./test_script.sh
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /home/s335105/test_script.sh.
Setting /home/s335105/test_script.sh to complain mode.

Before you begin, you may wish to check if a
profile already exists for the application you
wish to confine. See the following wiki page for
more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /home/s335105/test_script.sh

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
█
```

Запускаем программу `./test_script.sh`, получаем ошибки:

```
s335105@v132798:~$ ./test_script.sh
./test_script.sh: line 2: /usr/bin/mkdir: Permission denied
./test_script.sh: line 3: log/test.txt: Permission denied
./test_script.sh: line 4: /usr/bin/cat: Permission denied
./test_script.sh: line 5: /usr/bin/rm: Permission denied
s335105@v132798:~$
```

4) Запустите утилиту `aa-logprof` и настройте разрешения так, чтобы при выполнении программы не было ошибок. Запустите файл еще раз. Покажите, что теперь ошибок нет.

```
root@v132798:/home/s335105# aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/syslog.

Profile: /home/s335105/test_script.sh
Execute: /usr/bin/mkdir
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X)ix On / (D)eny / Abo(r)t / (F)inish

Profile: /home/s335105/test_script.sh
Execute: /usr/bin/mkdir
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X)ix On / (D)eny / Abo(r)t / (F)inish

Profile: /home/s335105/test_script.sh
Execute: /usr/bin/cat
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X)ix On / (D)eny / Abo(r)t / (F)inish

Profile: /home/s335105/test_script.sh
Execute: /usr/bin/rm
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X)ix On / (D)eny / Abo(r)t / (F)inish
```

В приведенных выше шагах нажимаем `(I)nherit`

```
Complain-mode changes:

Profile: /home/s335105/test_script.sh
Path: /dev/tty
New Mode: rw
Severity: 9

[1 - include <abstractions/consoles>]
2 - /dev/tty rw,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
Adding include <abstractions/consoles> to profile.
```

```
Profile: /home/s335105/test_script.sh
Path: /home/s335105/log/test.txt
New Mode: owner w
Severity: 6

[1 - owner /home/*/log/test.txt w,]
2 - owner /home/s335105/log/test.txt w,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
Adding owner /home/*/log/test.txt w, to profile.
```

```
Profile: /home/s335105/test_script.sh
Path: /etc/ld.so.cache
New Mode: r
Severity: 1

[1 - /etc/ld.so.cache r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
Adding /etc/ld.so.cache r, to profile.
```

```
Profile: /home/s335105/test_script.sh
Path: /proc/filesystems
New Mode: r
Severity: 6

[1 - /proc/filesystems r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
Adding /proc/filesystems r, to profile.
```

```
Profile: /home/s335105/test_script.sh
Path: /etc/locale.alias
New Mode: r
Severity: unknown

[1 - /etc/locale.alias r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
Adding /etc/locale.alias r, to profile.
```

```
Profile: /home/s335105/test_script.sh
Path: /home/s335105/log/test.txt
Old Mode: owner w
New Mode: owner r
Severity: 4

[1 - owner /home/*/log/test.txt r,]
2 - owner /home/s335105/log/test.txt r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)in
Adding owner /home/*/log/test.txt r, to profile.
```

Дальше во всех приведенных выше шагах нажимаем (A)llow

```
= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

[1 - /home/s335105/test_script.sh]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
Writing updated profile for /home/s335105/test_script.sh.
```

Нажимаем (S)ave Changes для сохранения изменений

```
s335105@v132798:~$ ./test_script.sh
Test file
s335105@v132798:~$
```

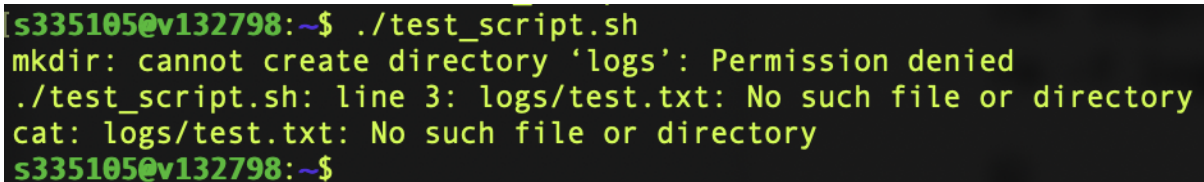
Программа успешно обрабатывает

5) В программе, измените местоположение создаваемого файла с /log на /logs.

Новый скрипт:

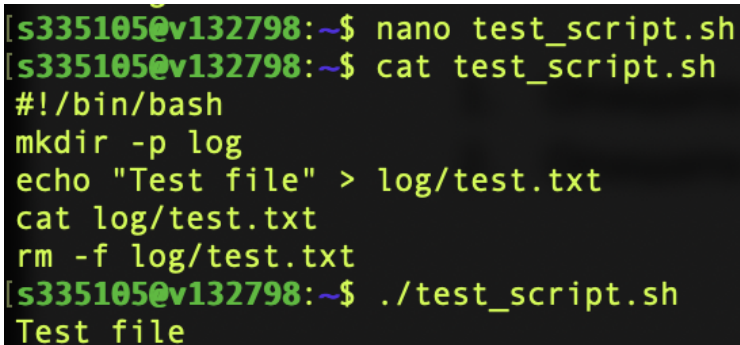
```
#!/bin/bash
mkdir -p logs
echo "Test file" > logs/test.txt
cat logs/test.txt
rm -f logs/test.txt
```

6) Создайте директорию logs. Запустите программу, покажите, что AppArmor блокирует попытку получить доступ к пути за пределами границ

A terminal window with a black background and green text. The user runs a script named test_script.sh. The script attempts to create a directory 'logs' and create a file 'logs/test.txt'. Both actions are blocked by AppArmor, resulting in 'Permission denied' and 'No such file or directory' errors. The prompt shows the user is s335105@v132798 in the home directory.

```
[s335105@v132798:~$ ./test_script.sh
mkdir: cannot create directory 'logs': Permission denied
./test_script.sh: line 3: logs/test.txt: No such file or directory
cat: logs/test.txt: No such file or directory
s335105@v132798:~$
```

7) Верните изначальное значение /log. Покажите, что программа работает корректно.

A terminal window with a black background and green text. The user uses nano to edit test_script.sh, changing the directory from 'logs' to 'log'. After running the script, it successfully creates the 'log' directory and the 'log/test.txt' file, and prints 'Test file'. The prompt shows the user is s335105@v132798 in the home directory.

```
[s335105@v132798:~$ nano test_script.sh
[s335105@v132798:~$ cat test_script.sh
#!/bin/bash
mkdir -p log
echo "Test file" > log/test.txt
cat log/test.txt
rm -f log/test.txt
[s335105@v132798:~$ ./test_script.sh
Test file
```

8) Отключите и удалите профиль безопасности из системы.

Отключить профиль можно с помощью команд:

```
# ln -s /etc/apparmor.d/home.s335105.test_script.sh
/etc/apparmor.d/disable/home.s335105.test_script.sh
```

```
apparmor_parser -R /etc/apparmor.d/home.s335105.test_script.sh
```

```
0 processes are in kill mode.  
[root@v132798:/home/s335105# aa-status | grep test_script.sh  
root@v132798:/home/s335105#
```

Как видно профиль больше не отражается в активных

Чтобы удалить профиль безопасности, нужно просто удалить профиль из `/etc/apparmor.d`:

```
rm -rf /etc/apparmor.d/home.s335105.test_script.sh
```