# MainPage/Info Security/Encript Lab 1.2

Университет ИТМО
Факультет ФПИ и КТ

## Отчёт по лабораторной работе 1.2

# «Политики безопасности Linux»

по дисциплину

**«Информационная безопасность»**

Студент: Чжоу Хунсян
Группа: P34131
Преподаватель:

Санкт-Петербург 2024

# Цель работы

Изучить параметры учетных записей пользователей в Linux. Ознакомиться с процессом конфигурации и изменения учетных записей по умолчанию. Изучить процесс разграничения доступа к данным и модификации прав доступа.

# Основная часть

1. Установите утилиту AppArmor
   `sudo apt install apparmor-utils apparmor-profiles`
   Напишите bash-скрипт который будет создавать файл в директории log , записывать в него что-то, читать из него и затем удалять.
2. Создайте директорию log. Выдайте файлу права на исполнение. Запустите файл, покажите вывод ./file
3. Создайте профиль безопасности для данной программы
   `sudo aa-genprof ./file`
   Покажите результат выполнения программы
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.
5. В программе, измените местоположение создаваемого файла с /log на /logs.
6. Создайте директорию logs. Запустите программу, покажите, что AppArmor блокирует попытку получить доступ к пути за пределами границ.
7. Верните изначальное значение /log. Покажите, что программа работает корректно.
8. Отключите и удалите профиль безопасности из системы.

# Выполнение

## 1. Установите утилиту AppArmor

```
parallels@ubuntu-linux-22-04-desktop:~$ sudo apt install apparmor-utils apparmor-profiles
[sudo] password for parallels:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 libllvm13 libwpe-1.0-1 libwpebackend-fdo-1.0-1
  linux-headers-5.15.0-112 linux-headers-5.15.0-112-generic
  linux-image-5.15.0-112-generic linux-modules-5.15.0-112-generic
  linux-modules-extra-5.15.0-112-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-apparmor python3-libapparmor
Suggested packages:
  vim-addon-manager
The following NEW packages will be installed:
  apparmor-profiles apparmor-utils python3-apparmor python3-libapparmor
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 202 kB of archives.
After this operation, 1546 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 python3-libapparmor ar
Get:2 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 python3-apparmor all 3
Get:3 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 apparmor-utils all 3.0
Get:4 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 apparmor-profiles all
Fetched 202 kB in 0s (507 kB/s)
Selecting previously unselected package python3-libapparmor.
(Reading database ... 241201 files and directories currently installed.)
Preparing to unpack .../python3-libapparmor_3.0.4-2ubuntu2.4_arm64.deb ...
Unpacking python3-libapparmor (3.0.4-2ubuntu2.4) ...
Selecting previously unselected package python3-apparmor.
Preparing to unpack .../python3-apparmor_3.0.4-2ubuntu2.4_all.deb ...
Unpacking python3-apparmor (3.0.4-2ubuntu2.4) ...
Selecting previously unselected package apparmor-utils.
Preparing to unpack .../apparmor-utils_3.0.4-2ubuntu2.4_all.deb ...
Unpacking apparmor-utils (3.0.4-2ubuntu2.4) ...
Selecting previously unselected package apparmor-profiles.
Preparing to unpack .../apparmor-profiles_3.0.4-2ubuntu2.4_all.deb ...
Unpacking apparmor-profiles (3.0.4-2ubuntu2.4) ...
```

```
Setting up python3-libapparmor (3.0.4-2ubuntu2.4) ...
Setting up apparmor-profiles (3.0.4-2ubuntu2.4) ...
Setting up python3-apparmor (3.0.4-2ubuntu2.4) ...
Setting up apparmor-utils (3.0.4-2ubuntu2.4) ...
Processing triggers for man-db (2.10.2-1) ...
```

## 2. Создайте директорию log. Выдайте файлу права на исполнение. Запустите файл, покажите вывод

```
parallels@ubuntu-linux-22-04-desktop:~$ nano file.sh
```

file:

```
#!/bin/bash

file="log/testfile.txt"

echo "This is a test file!" > $file

cat $file

rm -f $file
```

```
parallels@ubuntu-linux-22-04-desktop:~$ mkdir log
parallels@ubuntu-linux-22-04-desktop:~$ chmod +x file.sh
parallels@ubuntu-linux-22-04-desktop:~$ ./file.sh
This is a test file!
```

## 3. Создайте профиль безопасности для данной программы

Создать профиль безопасности

```
parallels@ubuntu-linux-22-04-desktop:~$ sudo aa-genprof ./file
```

Получается профиль в /etc/apparmor.d так:

```
# Last Modified: Mon Dec 16 15:59:40 2024
abi <abi/3.0>,

include <tunables/global>

/home/parallels/file {
  include <abstractions/base>
  include <abstractions/bash>
  include <abstractions/consoles>

  /home/parallels/file r,
  /usr/bin/bash ix,
  owner /home/parallels/log/testfile.txt rw,

}
```

Запустить file.sh

```
parallels@ubuntu-linux-22-04-desktop:~$ ./file
./file: line 7: /usr/bin/cat: Permission denied
./file: line 9: /usr/bin/rm: Permission denied
```

**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.**

```
parallels@ubuntu-linux-22-04-desktop:~$ sudo aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/syslog.

Profile:  /home/parallels/file
Execute:  /usr/bin/cat
Severity: unknown

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

Profile:  /home/parallels/file
Execute:  /usr/bin/cat
Severity: unknown

(I)nherit / (C)hild Inherit / (N)amed Inherit / (X) ix Off / (D)eny / Abo(r)t / (F)inish
Complain-mode changes:
Enforce-mode changes:

Profile:  /home/parallels/file
Path:     /usr/bin/cat
New Mode: ix
Severity: unknown

 [1 - /usr/bin/cat ix,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)
Adding /usr/bin/cat ix, to profile.

Profile:  /home/parallels/file
Path:     /usr/bin/rm
New Mode: ix
Severity: unknown

 [1 - /usr/bin/rm ix,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)
Adding /usr/bin/rm ix, to profile.

= Changed Local Profiles =

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

```
 [1 - /home/parallels/file]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean pro
Writing updated profile for /home/parallels/file.
```

```
# Last Modified: Mon Dec 16 16:01:11 2024
abi <abi/3.0>,

include <tunables/global>

/home/parallels/file {
  include <abstractions/base>
  include <abstractions/bash>
  include <abstractions/consoles>

  /home/parallels/file r,
  /usr/bin/bash ix,
  /usr/bin/cat ir,
  /usr/bin/rm ir,
  owner /home/parallels/log/testfile.txt rw,
}
```

```
parallels@ubuntu-linux-22-04-desktop:~$ ./file
This is a test file!
```

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

```
parallels@ubuntu-linux-22-04-desktop:~$ nano file
```

file

```
#!/bin/bash

file="logs/testfile.txt"

echo "This is a test file!" > $file

cat $file

rm -f $file
```

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

```
parallels@ubuntu-linux-22-04-desktop:~$ mkdir logs
parallels@ubuntu-linux-22-04-desktop:~$ ./file
./file: line 5: logs/testfile.txt: Permission denied
cat: logs/testfile.txt: No such file or directory
```

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

```
parallels@ubuntu-linux-22-04-desktop:~$ nano file
```

file

```
#!/bin/bash

file="log/testfile.txt"

echo "This is a test file!" > $file

cat $file

rm -f $file
```

```
parallels@ubuntu-linux-22-04-desktop:~$ ./file
This is a test file!
```

## 8. Отключите и удалите профиль безопасности из системы.

```
parallels@ubuntu-linux-22-04-desktop:~$ sudo aa-disable ./file
Disabling /home/parallels/file.
```

```
parallels@ubuntu-linux-22-04-desktop:/etc/apparmor.d$ cd /etc/apparmor.d
parallels@ubuntu-linux-22-04-desktop:/etc/apparmor.d$ sudo rm -f home.parallels.file
```

# Вывод

## Заключение

В рамках лабораторной работы №2 были изучены основы политики безопасности AppArmor в системе Linux. Выполнив установку и настройку AppArmor, мы научились создавать профили безопасности для приложений, контролировать доступ к файлам и путям, а также диагностировать и устранять ошибки безопасности. Работая с `aa-genprof` и `aa-logprof`, мы улучшили управление разрешениями и наблюдали, как AppArmor помогает защищать системы от несанкционированного доступа и эксплуатации. Умение применять эти инструменты поможет в создании более безопасных и стабильных серверных систем.