ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет Программной Инженерии и Компьютерной Техники

Дисциплина:
«*Информационная безопасность*»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2
«Политики безопасности Linux»

Вариант 9

Выполнил:
Студент гр. P34151
Соловьев Артемий Александрович

Преподаватель:
Маркина Татьяна Анатольевна

Санкт-Петербург
2024г.

Задание:

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.

Дополнительная часть:

1. Опишите отличия SELinux vs AppArmor?
2. Опишите режимы профилей Enforce и Complain? Их различия для чего нужны?

Выполнение

Установка утилиты AppArmor

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ sudo apt install apparmor-utils apparmor
-profiles
[sudo] password for artemiy:
Reading package lists... Done
```

Bash-скрипт для создания, записи, чтения и удаления файла в директории log

Команды для создания

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ nano file.sh
artemiy@artemiy-QEMU-Virtual-Machine:~$ ls
Desktop    Downloads  Music     Public     Videos
Documents  file.sh    Pictures  Templates
artemiy@artemiy-QEMU-Virtual-Machine:~$
```

Содержимое файла file.sh

```
#! /bin/bash

touch ./log/file.txt

echo "test text" > ./log/file.txt

cat ./log/file.txt

rm ./log/file.txt

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

Создание директории log, выдача прав на исполнения для bash-скрипта и его исполнение

Создадим директорию /log.

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ mkdir log
artemiy@artemiy-QEMU-Virtual-Machine:~$ ls
Desktop    Downloads  log       Pictures  Templates
Documents  file.sh    Music     Public    Videos
artemiy@artemiy-QEMU-Virtual-Machine:~$
```

Выдадим права на исполнения файла file.sh

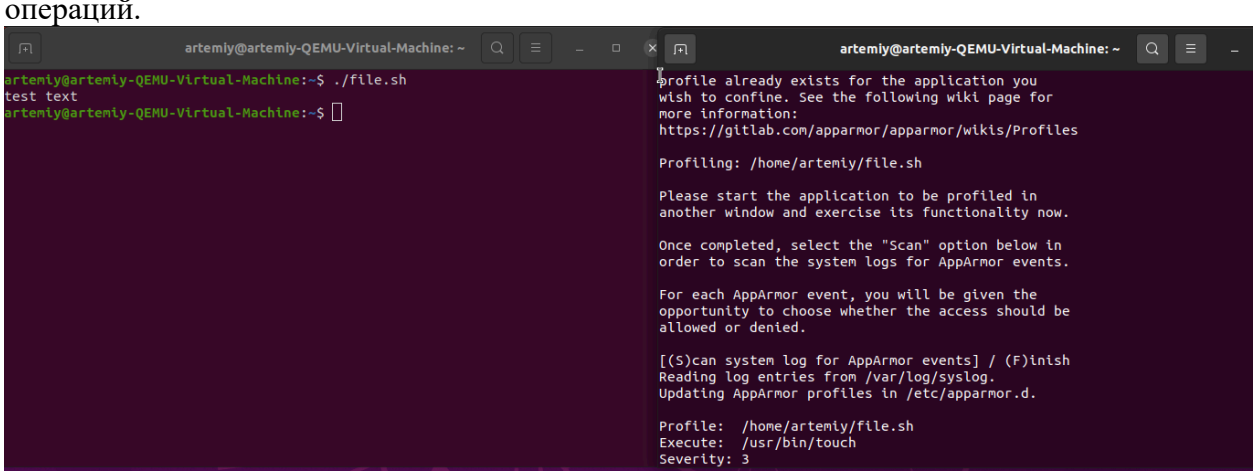
```
artemiy@artemiy-QEMU-Virtual-Machine:~$ chmod +x file.sh
artemiy@artemiy-QEMU-Virtual-Machine:~$ ls -la
total 80
drwxr-xr-x 16 artemiy artemiy 4096 дек  9 16:31 .
drwxr-xr-x  3 root    root    4096 дек  7 15:29 ..
-rw-r--r--  1 artemiy artemiy  220 дек  7 15:29 .bash_logout
-rw-r--r--  1 artemiy artemiy 3771 дек  7 15:29 .bashrc
drwxrwxr-x 13 artemiy artemiy 4096 дек  7 15:37 .cache
drwx------ 12 artemiy artemiy 4096 дек  7 15:39 .config
drwxr-xr-x  2 artemiy artemiy 4096 дек  7 15:34 Desktop
drwxr-xr-x  2 artemiy artemiy 4096 дек  7 15:34 Documents
drwxr-xr-x  3 artemiy artemiy 4096 дек  7 15:40 Downloads
-rwxrwxr-x  1 artemiy artemiy  109 дек  9 16:28 file.sh
```

Запустим скрипт и проверим вывод

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ ./file.sh
test text
artemiy@artemiy-QEMU-Virtual-Machine:~$ ls ./log/
artemiy@artemiy-QEMU-Virtual-Machine:~$
```

Создание профиля безопасности для file.sh

При выполнении команды *sudo aa-genprof ./file.sh* мы видим такое окно с логами операций.



Пробуем запустить файл file.sh

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ ./file.sh
./file.sh: line 3: /usr/bin/touch: Permission denied
./file.sh: line 7: /usr/bin/cat: Permission denied
./file.sh: line 9: /usr/bin/rm: Permission denied
```

Настройка разрешений через aa-logprof

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ sudo aa-logprof
Reading log entries from /var/log/syslog.
Updating AppArmor profiles in /etc/apparmor.d.

Profile:  /home/artemiy/file.sh
Execute:  /usr/bin/touch
Severity: 3

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

Profile:  /home/artemiy/file.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/artemiy/file.sh
Execute:  /usr/bin/rm
Severity: unknown

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

На скриншоте выше мы выдали разрешения для файла
Проверка, что разрешения выданы:

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ ./file.sh
test text
```

Изменение метаположения создаваемого файла на /logs

```
#! /bin/bash

touch ./logs/file.txt

echo "test text" > ./logs/file.txt

cat ./logs/file.txt

rm ./logs/file.txt
```

[Read 11 lines]

Создание директории logs и запуск программы

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ ./file.sh
touch: cannot touch './logs/file.txt': Permission denied
./file.sh: line 5: ./logs/file.txt: Permission denied
cat: ./logs/file.txt: No such file or directory
rm: cannot remove './logs/file.txt': No such file or directory
artemiy@artemiy-QEMU-Virtual-Machine:~$
```

Ожидаемо, доступ заблокирован.

Возвращаем скрипт в начальный вид

nano file.txt

```
#! /bin/bash

touch ./log/file.txt

echo "test text" > ./log/file.txt

cat ./log/file.txt

rm ./log/file.txt
```

Проверяем работоспособность скрипта

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ ./file.sh
test text
artemiy@artemiy-QEMU-Virtual-Machine:~$
```

Отключение и удаления профиля безопасности

```
artemiy@artemiy-QEMU-Virtual-Machine:~$ sudo aa-disable /etc/apparmor.d/home.artemiy.file.sh
Disabling /etc/apparmor.d/home.artemiy.file.sh.
artemiy@artemiy-QEMU-Virtual-Machine:~$ sudo rm /etc/apparmor.d/home.artemiy.file.sh
artemiy@artemiy-QEMU-Virtual-Machine:~$ ls /etc/apparmor.d/
abi                 sbin.syslog-ng                  usr.sbin.dnsmasq
abstractions        tunables                        usr.sbin.identd
apache2.d           ubuntu_pro_apt_news             usr.sbin.ippusbxd
bin.ping            ubuntu_pro_esm_cache            usr.sbin.mdnsd
disable             usr.bin.chromium-browser        usr.sbin.nmbd
force-complain      usr.bin.evince                  usr.sbin.nscd
local               usr.bin.firefox                 usr.sbin.rsyslogd
lsb_release         usr.bin.man                     usr.sbin.smbd
nvidia_modprobe     usr.lib.snapd.snap-confine.real usr.sbin.smbldap-useradd
sbin.dhclient       usr.sbin.avahi-daemon           usr.sbin.tcpdump
sbin.klogd          usr.sbin.cups-browsed           usr.sbin.traceroute
sbin.syslogd        usr.sbin.cupsd
artemiy@artemiy-QEMU-Virtual-Machine:~$ ./file.sh
test text
artemiy@artemiy-QEMU-Virtual-Machine:~$
```

Дополнительная часть

Отличия SELinux vs AppArmor

Критерий	SELinux	AppArmor
Контроль доступа	Использует профили безопасности на основе меток файлов	Использует профили безопасности, основанные на путях
Сложность в освоении	Сложная настройка и администрирование	Простая настройка и администрирование
Требуется сложная конфигурация	Да	Нет
Влияние на производительность	Из-за сложных проверок может несильно замедлить систему	Небольшое влияние во время запуска

Режимы профилей Enforce и Complain. Сравнение и для чего нужны

Режим профиля определяет обработку правил во время выполнения, если произойдет соответствующее событие.

Описание профилей

1. Enforce:
   Система применяет правила, сообщает о нарушении и записывает его в системный журнал.
   Мы используем этот режим, чтобы запретить программе выполнять определенные вызовы.
2. Complain: Система не применяет правила, но записывает нарушения в журнал.

Для чего нужны

1. Enforce:
   Используется, чтобы запретить программе выполнять определенные вызовы
2. Complain:
   Этот режим полезен, если мы хотим обнаружить вызовы, которые делает программа

Вывод

В ходе выполнения лабораторной работы были созданы (а в последствии удалены) политики безопасности по средствам утилиты AppArmor, а также была проведена сравнительная характеристика AppArmor и SELinux.