Отчет по лабораторной работе
“Политики безопасности Linux”
по дисциплине
“Информационная безопасность”

Выполнил:
студент группы P34131
Бусыгин Дмитрий Алексеевич
Преподаватель:
Маркина Татьяна Анатольевна

Санкт-Петербург
2024

Цель работы

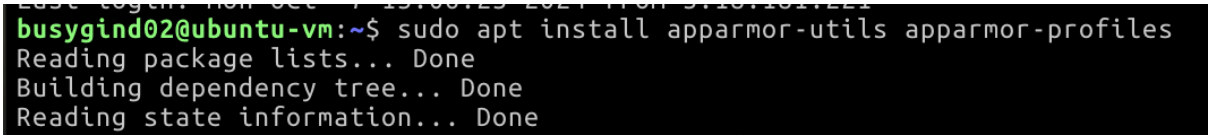
Изучить принципы работы утилиты AppArmor и сравнить её с утилитой SELinux

Основная часть

Пункт 1.

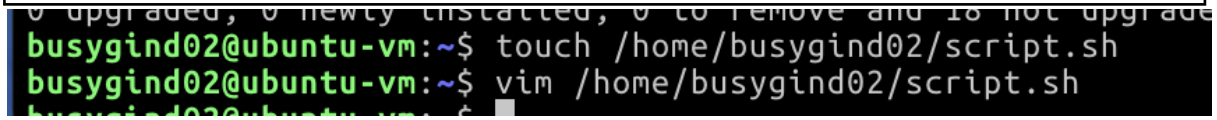
Установка AppArmor.

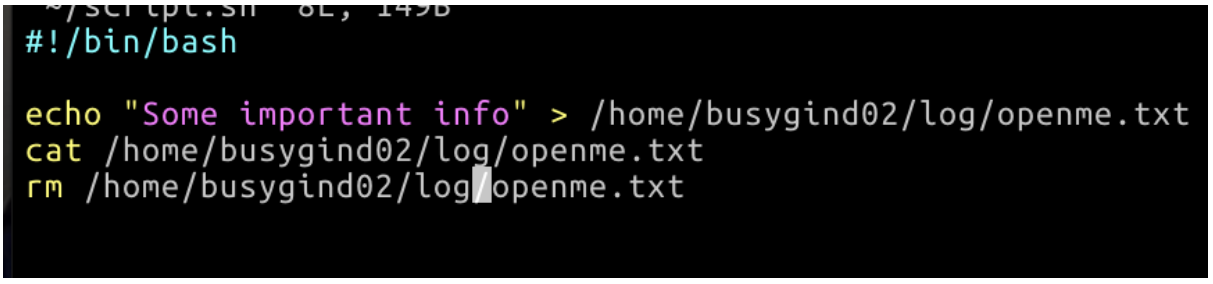
```
busygind02@ubuntu-vm:~$ sudo apt install apparmor-utils apparmor-profiles
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
...
```



Создание bash-скрипта для манипуляции файлом

```
busygind02@ubuntu-vm:~$ touch /home/busygind02/script.sh
busygind02@ubuntu-vm:~$ vim /home/busygind02/script.sh
#!/bin/bash

echo "Some important info" > /home/busygind02/log/openme.txt
cat /home/busygind02/log/openme.txt
rm /home/busygind02/log/openme.txt
~
-- INSERT --
```





Пункт 2.

Создание директории log, выдача прав и запуск скрипта

```
busygind02@ubuntu-vm:~$ mkdir log
busygind02@ubuntu-vm:~$ chmod a+x script.sh
busygind02@ubuntu-vm:~$ ls -l
total 8
drwxr-xr-x 2 busygind02 busygind02 4096 Oct  6 20:51 log
-rwxr-xr-x 1 busygind02 busygind02  149 Oct  6 20:49 script.sh
```

```
busygind02@ubuntu-vm:~$ ./script.sh
Some important info
```

```
busygind02@ubuntu-vm:~$ mkdir log
busygind02@ubuntu-vm:~$ chmod a+x script.sh
busygind02@ubuntu-vm:~$ ls -l
total 8
drwxr-xr-x 2 busygind02 busygind02 4096 Oct  6 20:51 log
-rwxr-xr-x 1 busygind02 busygind02  149 Oct  6 20:49 script.sh
busygind02@ubuntu-vm:~$ ./script.sh
Some important info
```

Пункт 3.

Создание профиля безопасности

```
busygind02@ubuntu-vm:~$ sudo aa-genprof ./script.sh
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /home/busygind02/script.sh.
Setting /home/busygind02/script.sh to complain mode.
...
Finished generating profile for /home/busygind02/script.sh.
busygind02@ubuntu-vm:~$ ./script.sh
./script.sh: line 3: /home/busygind02/log/openme.txt: Permission denied
./script.sh: line 4: /usr/bin/cat: Permission denied
./script.sh: line 5: /usr/bin/rm: Permission denied
```

```
busygind02@ubuntu-vm:~$ sudo aa-genprof ./script.sh
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /home/busygind02/script.sh.
Setting /home/busygind02/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/busygind02/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
Setting /home/busygind02/script.sh to enforce mode.

Reloaded AppArmor profiles in enforce mode.

Please consider contributing your new profile!
See the following wiki page for more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Finished generating profile for /home/busygind02/script.sh.
busygind02@ubuntu-vm:~$
```

Видим, что у скрипта перестало хватать прав на манипуляции с файлом

Пункт 4.

Дополнительная настройка профиля безопасности

```
busygind02@ubuntu-vm:~$ sudo aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
```

```
Reading log entries from /var/log/syslog.

Profile:  /home/busygind02/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/busygind02/script.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:
Enforce-mode changes:

Profile:  /home/busygind02/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

Profile:  /home/busygind02/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/busygind02/script.sh
Path:     /home/busygind02/log/openme.txt
New Mode: owner w
Severity: 6
 [1 - owner /home/*/log/openme.txt w,]
  2 - owner /home/busygind02/log/openme.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

Profile:  /home/busygind02/script.sh
Path:     /home/busygind02/log/openme.txt
New Mode: owner w
Severity: 6
  1 - owner /home/*/log/openme.txt w,
 [2 - owner /home/busygind02/log/openme.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/busygind02/log/openme.txt w, to profile.
```

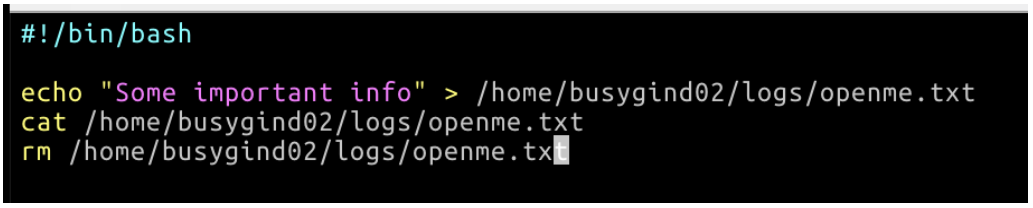
```
= Changed Local Profiles =

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

 [1 - /home/busygind02/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/busygind02/script.sh.
busygind02@ubuntu-vm:~$ sudo aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/syslog.
Complain-mode changes:
Enforce-mode changes:

Profile:  /home/busygind02/script.sh
Path:     /home/busygind02/log/openme.txt
Old Mode: owner w
New Mode: owner rw
Severity: 6
 [1 - owner /home/*/log/openme.txt rw,]
  2 - owner /home/busygind02/log/openme.txt rw,
(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

Profile:  /home/busygind02/script.sh
Path:     /home/busygind02/log/openme.txt
Old Mode: owner w
New Mode: owner rw
Severity: 6
  1 - owner /home/*/log/openme.txt rw,
 [2 - owner /home/busygind02/log/openme.txt rw,]
(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/busygind02/log/openme.txt rw, to profile.
Deleted 1 previous matching profile entries.

= Changed Local Profiles =

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

 [1 - /home/busygind02/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/busygind02/script.sh.
```

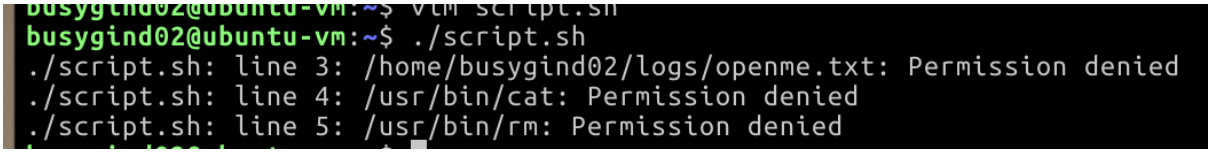
В логи AppArmor записались ошибки доступа к каким либо ресурсам в системе. Прямо внутри утилиты из можно “резолвить”, т.е. выбирать действия по изменению/игнорированию прав тех или иных профилей

Пункты 5-6.

Проверка доступа до иных путей

```
busygind02@ubuntu-vm:~$ mkdir logs
busygind02@ubuntu-vm:~$ vim script.sh
#!/bin/bash

echo "Some important info" > /home/busygind02/logs/openme.txt
cat /home/busygind02/logs/openme.txt
rm /home/busygind02/logs/openme.txt
busygind02@ubuntu-vm:~$ ./script.sh
./script.sh: line 3: /home/busygind02/logs/openme.txt: Permission denied
./script.sh: line 4: /usr/bin/cat: Permission denied
./script.sh: line 5: /usr/bin/rm: Permission denied
```



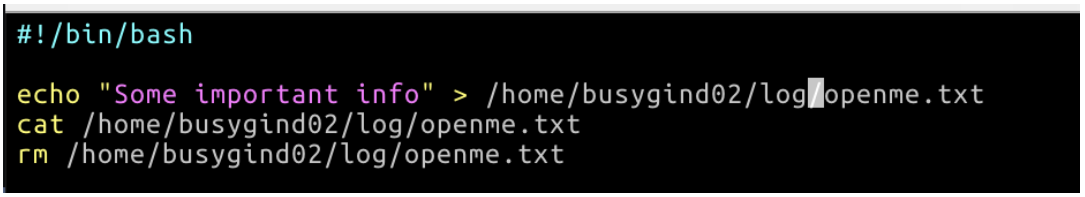


Видим, что доступа нет, что и закономерно, т.к. директория logs не указана в профиле в файле /etc/apparmor.d/home.busygind02.script.sh

Пункт 7.

Повторная проверка

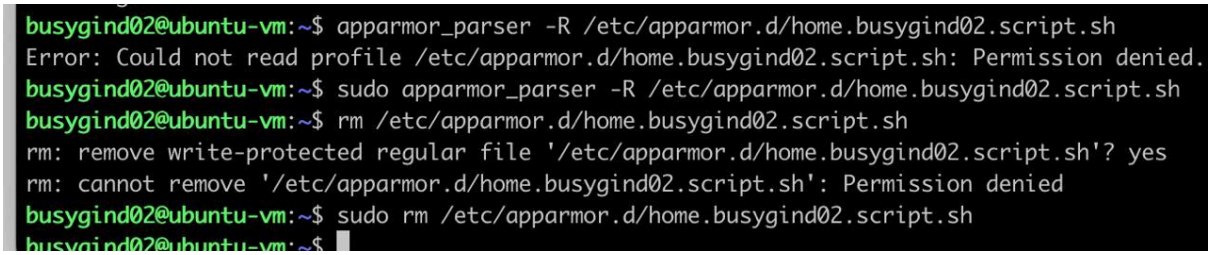
```
busygind02@ubuntu-vm:~$ vim script.sh
#!/bin/bash

echo "Some important info" > /home/busygind02/log/openme.txt
cat /home/busygind02/log/openme.txt
rm /home/busygind02/log/openme.txt
busygind02@ubuntu-vm:~$ ./script.sh
Some important info
```



Пункт 8.

Удаление профиля безопасности

```
busygind02@ubuntu-vm:~$ sudo apparmor_parser -R /etc/apparmor.d/home.busygind02.script.sh
busygind02@ubuntu-vm:~$ sudo rm /etc/apparmor.d/home.busygind02.script.sh
```



Дополнительная часть

Вопрос 1: опишите отличия SELinux vs AppArmor?

1. **Модель контроля безопасности**:

- **SELinux** работает на основе меток, все файлы и процессы маркируются, а доступ контролируется на основе политики, определяющей, какие метки могут взаимодействовать друг с другом.
- **AppArmor** использует модель безопасности на основе профилей, где каждому приложению назначается профиль в `/etc/apparmor.d`, определяющий его разрешения и ограничения.

2. **Политики**:

- **SELinux** имеет более сложные и конкретизированные политики, которые могут контролировать доступ на уровне элементов, таких как системные вызовы и файлы. Политики SELinux пишутся на специальном языке и, на мой взгляд, достаточно сложны в настройке и управлении.
- **AppArmor** имеет более простые и менее подробные политики, зачастую определяемые на уровне системы файлов и не требуют знания сложных языков. Это делает AppArmor более простым в использовании для многих администраторов.

Вопрос 2: опишите режимы профилей Enforce и Complain? Их различия для чего нужны?

Enforce и Complain - это режимы управления политиками безопасности в AppArmor.

- **Enforce mode** по сути реализует презумпцию запрета, т.е. все действия, которые не разрешены явно - запрещены. Применять его стоит при необходимости непосредственной защиты системы, т.е. уже в проде.

- **Complain mode** не блокирует выполнение действий, но логирует все неописанные в профилях действия в системных журналах как предупреждения. Его удобно применять на этапах разработки и тестирования, чтобы отследить какие права на самом деле нужны пользователям