UNIX
Лабораторная работа №2
Политики безопасности Linux

ФИО студента: Готовко Алексей Владимирович
Учебная группа: P34101

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.

Выполнение работы

Основная часть

Пункт 1

Задание:

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.

```
xgodness@xgodness-pc:~/infosec$ sudo apt install apparmor-utils apparmor-profiles
[sudo] password for xgodness:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
<...>
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) ...
xgodness@xgodness-pc:~/infosec$
```

`file`:

```
#!/bin/bash
touch log/testfile
echo "Pancake is a natural born killer" > log/testfile
cat log/testfile
rm log/testfile
```

Пункт 2

Задание:

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

```
xgodness@xgodness-pc:~/infosec$ mkdir log
xgodness@xgodness-pc:~/infosec$ sudo chmod u+x file
xgodness@xgodness-pc:~/infosec$ ls -l | grep file
-rwxrw-r-- 1 xgodness xgodness  123 Oct 17 19:10 file
xgodness@xgodness-pc:~/infosec$ ./file
Pancake is a natural born killer
xgodness@xgodness-pc:~/infosec$
```

Пункт 3

Задание:

Создайте профиль безопасности для данной программы (`sudo aa-genprof file`). Покажите результат выполнения программы.

```
xgodness@xgodness-pc:~/infosec$ sudo aa-genprof file
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /home/xgodness/infosec/file.
Setting /home/xgodness/infosec/file 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/xgodness/infosec/file

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/xgodness/infosec/file 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/xgodness/infosec/file.
```

```
xgodness@xgodness-pc:~/infosec$ ./file
./file: line 2: /usr/bin/touch: Permission denied
./file: line 3: log/testfile: Permission denied
./file: line 4: /usr/bin/cat: Permission denied
./file: line 5: /usr/bin/rm: Permission denied
xgodness@xgodness-pc:~/infosec$
```

Пункт 4

Задание:

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

```
xgodness@xgodness-pc:~/infosec$ sudo aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/syslog.

Profile:  /home/xgodness/infosec/file
Execute:  /usr/bin/touch
Severity: 3

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

>>> I

Profile:  /home/xgodness/infosec/file
Execute:  /usr/bin/cat
Severity: unknown

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

>>> I

Profile:  /home/xgodness/infosec/file
Execute:  /usr/bin/rm
Severity: unknown

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

>>> I

Enforce-mode changes:

Profile:  /home/xgodness/infosec/file
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

>>> A

Profile:  /home/xgodness/infosec/file
Path:     /home/xgodness/infosec/log/testfile
New Mode: owner rw
Severity: 6

 [1 - owner /home/*/infosec/log/testfile rw,]
  2 - owner /home/xgodness/infosec/log/testfile 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

>>> ARROW DOWN

Profile:  /home/xgodness/infosec/file
Path:     /home/xgodness/infosec/log/testfile
New Mode: owner rw
Severity: 6

  1 - owner /home/*/infosec/log/testfile rw,
 [2 - owner /home/xgodness/infosec/log/testfile 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

>>> A

Adding owner /home/xgodness/infosec/log/testfile rw, to profile.

= Changed Local Profiles =

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

 [1 - /home/xgodness/infosec/file]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t

>>> S

Writing updated profile for /home/xgodness/infosec/file.
xgodness@xgodness-pc:~/infosec$
```

```
xgodness@xgodness-pc:~/infosec$ ./file
Pancake is a natural born killer
xgodness@xgodness-pc:~/infosec$
```

Пункт 5

Задание:
В программе измените местоположение создаваемого файла с `log` на `logs`.

```
xgodness@xgodness-pc:~/infosec$ cat file
#!/usr/bin/bash
touch logs/testfile
echo "Pancake is a natural born killer" > logs/testfile
cat logs/testfile
rm logs/testfile
xgodness@xgodness-pc:~/infosec$
```

Пункт 6

Задание:

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

```
xgodness@xgodness-pc:~/infosec$ mkdir logs
xgodness@xgodness-pc:~/infosec$ ./file
touch: cannot touch 'logs/testfile': Permission denied
./file: line 3: logs/testfile: Permission denied
cat: logs/testfile: No such file or directory
rm: cannot remove 'logs/testfile': No such file or directory
xgodness@xgodness-pc:~/infosec$
```

Пункт 7

Задание:

Верните изначальное значение `log`. Покажите, что программа работает корректно.

```
xgodness@xgodness-pc:~/infosec$ cat file
#!/usr/bin/bash
touch log/testfile
echo "Pancake is a natural born killer" > log/testfile
cat log/testfile
rm log/testfile
xgodness@xgodness-pc:~/infosec$ ./file
Pancake is a natural born killer
xgodness@xgodness-pc:~/infosec$
```

Пункт 8

Задание:

Отключите и удалите профиль безопасности из системы.

```
xgodness@xgodness-pc:~/infosec$ sudo aa-disable /etc/apparmor.d/home.xgodness.infosec.file
Disabling /etc/apparmor.d/home.xgodness.infosec.file.
xgodness@xgodness-pc:~/infosec$ sudo apparmor_parser -R /etc/apparmor.d/home.xgodness.infosec.file
xgodness@xgodness-pc:~/infosec$ sudo rm /etc/apparmor.d/home.xgodness.infosec.file
```

Дополнительная часть

Пункт 1

Задание:
Опишите отличия `SELinux` vs `AppArmor`.

`SELinux` (Security-Enhanced Linux) и `AppArmor` — два механизма контроля доступа, которые обеспечивают защиту операционных систем Linux.

Основные отличия:

- `SELinux` использует контекстно-зависимую модель безопасности (mandatory access control, MAC). В ней все файлы и процессы имеют метки безопасности (контексты), и политика безопасности основана на этих контекстах. Это более строгая модель, требующая тщательной настройки.
  `AppArmor` использует модель на основе профилей. Для каждого приложения создается профиль, который определяет, какие файлы и ресурсы система разрешает использовать этому приложению.

- `SELinux` предоставляет более гибкие возможности контроля за системой, но эта гибкость требует сложной настройки и глубокого понимания системы безопасности. Политики `SELinux` могут быть довольно сложными.
  `AppArmor` легче настроить и использовать, так как профили более просты и специфичны для приложений.

- `SELinux` использует метки безопасности (`labels`), которые прикрепляются к файлам и процессам, и на их основе система решает, можно ли процессу получить доступ к файлу.
  `AppArmor` использует профили на основе путей (`path-based`), где контроль доступа осуществляется по имени файлов, к которым пытается обратиться приложение.

Пункт 2

Задание:
Опишите режимы профилей `Enforce` и `Complain` и их различия. Для чего они нужны?

`Enforce` и `Complain` — это два режима работы профилей `AppArmor`, которые позволяют управлять поведением приложений в системе.

В режиме `Enforce` `AppArmor` активно применяет политику безопасности профиля. Это означает, что если приложение пытается выполнить действие, не разрешённое профилем, это действие будет заблокировано. Используется для строгого контроля приложений и защиты системы от выполнения запрещённых действий.

В режиме `Complain` `AppArmor` не блокирует действия, которые нарушают политику профиля, а записывает информацию о них в журнал. Используется для отладки профилей безопасности. Позволяет администратору увидеть, какие действия были бы заблокированы в режиме `Enforce`, и скорректировать профиль перед его активацией в строгом режиме.

Как правило, режим `Complain` используется для диагностики и отладки профилей до их перевода в строгий режим `Enforce`, который уже активно контролирует поведение приложений.