ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Дисциплина:

«Операционные системы»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 8

Apparmor/SELinux

Выполнила:

Студентка гр. №N3253

Пастухова А.А.

Проверил:

Ханов А.Р.

Санкт-Петербург

2022 г.

Задачи:

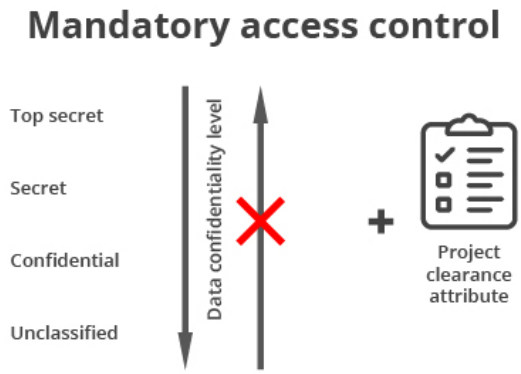
Обе

1. Настроить Apparmor для мониторинга сложного приложения и продемонстрировать его работу при ограниченных правах (оконное приложение или веб-сервер)
2. Настроить selinux в режиме мандатного доступа (CentOS и др.) и продемонстрировать работу в двухуровневой модели.

Ход работы:

AppArmor — это реализация Модуля безопасности линукс по управлению доступом на основе имен. AppArmor ограничивает отдельные программы набором перечисленных файлов и возможностями в соответствии с правилами Posix 1003.1e. Модель безопасности Apparmor заключается в привязке атрибутов контроля доступа не к пользователям, а к программам. AppArmor обеспечивает изоляцию с помощью профилей, загружаемых в ядро, как правило, при загрузке.

Так же, как и SELinux AppArmor является реализацией системы Mandatory Access Control (MAC), основанной на архитектуре Linux Security Modules (LSM).



Для каждой программы, которую нужно контролировать создается файл профиля, если его нет или он отключен, программа выполняется без ограничений. Это гарантирует, стабильную работу системы и позволяет контролировать работу программ. Профили могут работать в двух режимах:

Enforce - ядро гарантирует соблюдение правил, указанных в файле профиля, все нарушения блокируются, а также записываются в файл журнала, где могут быть очень легко просмотрены.

Complain - режим обучения, программа будет только регистрировать нарушения ничего не блокируя.

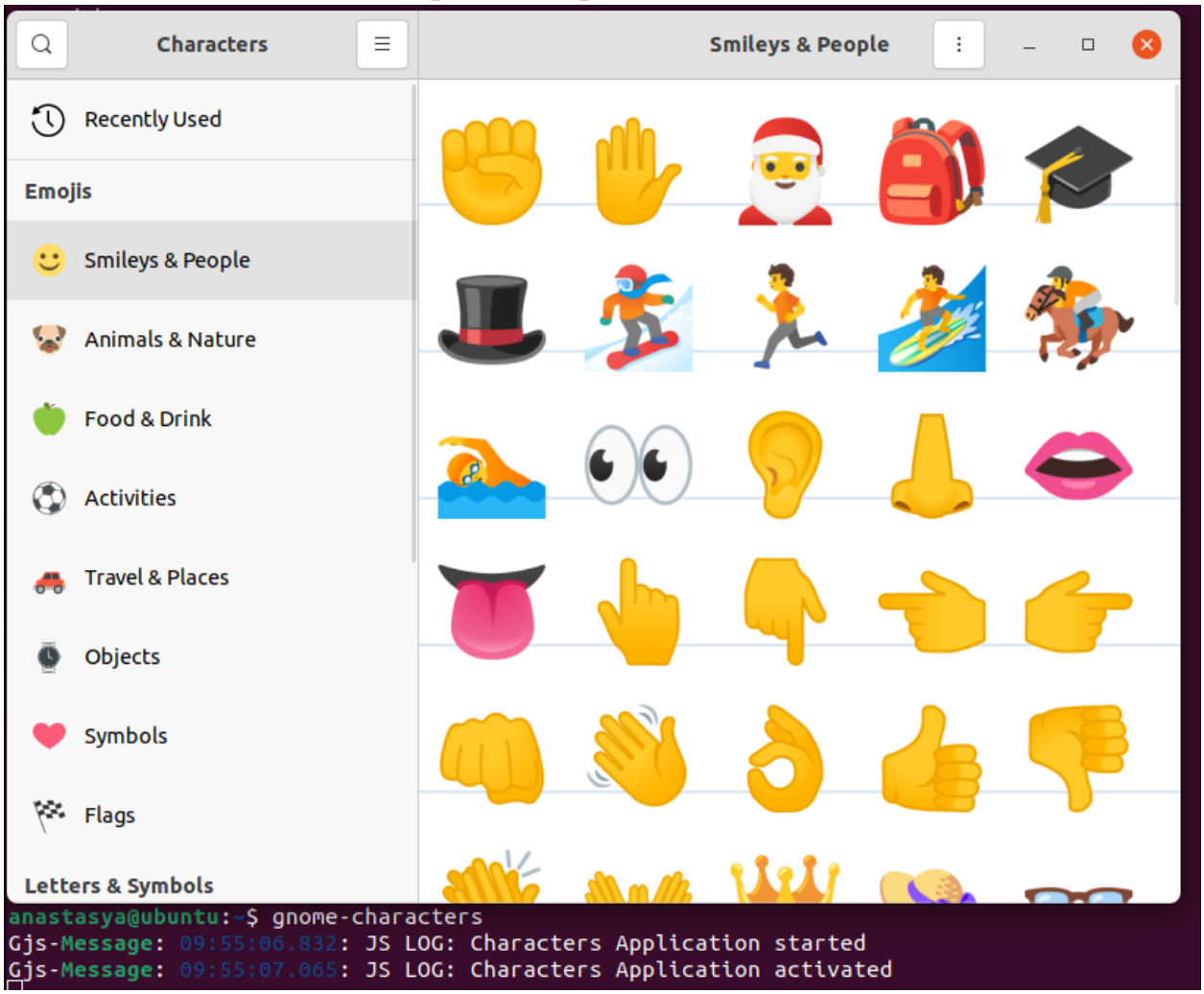
Установка модуля

```
anastasya@ubuntu:~$ sudo apt install apparmor-utils apparmor-profiles
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apparmor-profiles is already the newest version (3.0.3-0ubuntu1).
The following additional packages will be installed:
  python3-apparmor python3-libapparmor
Suggested packages:
```

Узнаем статус и видим 56 загруженных профилей, где 36 из них находятся в режиме ограничения, а 15 в режиме обучения.

```
anastasya@ubuntu:~$ sudo apparmor_status
apparmor module is loaded.
51 profiles are loaded.
36 profiles are in enforce mode.
   /snap/core/13308/usr/lib/snapd/snap-confine
   /snap/core/13308/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/bin/evince
   /usr/bin/evince-previewer
   /usr/bin/evince-previewer//sanitized_helper
   /usr/bin/evince-thumbnailer
   /usr/bin/evince//sanitized_helper
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/lib/snapd/snap-confine
   /usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/sbin/cups-browsed
   /usr/sbin/cupsd
   /usr/sbin/cupsd//third_party
   /{,usr/}sbin/dhclient
   docker-default
15 profiles are in complain mode.
   avahi-daemon
   dnsmasq
   dnsmasq//libvirt_leaseshelper
   identd
   klogd
   mdnsd
   nmbd
   nscd
   ping
   smbd
   smbldap-useradd
   smbldap-useradd///etc/init.d/nscd
   syslog-ng
   syslogd
   traceroute
0 profiles are in kill mode.
0 profiles are in unconfined mode.
2 processes have profiles defined.
2 processes are in enforce mode.
   /usr/sbin/cups-browsed (1583)
   /usr/sbin/cupsd (1485)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
anastasya@ubuntu:~$
```

Буду тестировать с помощью GNOME Characters - таблицы символов Юникода. Является частью рабочей среды GNOME.



Создаем профиль

```
anastasya@ubuntu:~$ sudo aa-autodep gnome-text-editor
Writing updated profile for /usr/bin/gedit.
```

```
anastasya@ubuntu:~$ sudo aa-autodep gnome-characters
Writing updated profile for /usr/share/org.gnome.Characters/org.gnome.Characters.
```

Еще раз проверяем статус и видим , что добавился новый профиль в режиме complain

```
17 profiles are in complain mode.
   /usr/bin/gedit
   /usr/share/org.gnome.Characters/org.gnome.Characters
   avahi-daemon
   dnsmasq
```

Переключим в enforce режим

```
anastasya@ubuntu:~$ sudo aa-enforce gnome-characters
Setting /usr/share/org.gnome.Characters/org.gnome.Characters to enforce mode.
```

Попытаемся открыть таблицу символов - невозможно

```
anastasya@ubuntu:~$ gnome-characters

(org.gnome.Characters:8831): Gjs-CRITICAL **: 09:59:05.705: JS ERROR: ImportError: No JS module '
main' found in search path
@/usr/bin/gnome-characters:6:1


(org.gnome.Characters:8831): Gjs-CRITICAL **: 09:59:05.705: Script /usr/bin/gnome-characters thre
w an exception
```

Смотрим созданный профиль

```
anastasya@ubuntu:~$ sudo cat /etc/apparmor.d/usr.share.org.gnome.Characters.org.gnome.Characters
# Last Modified: Fri Jun 24 09:57:29 2022
abi <abi/3.0>,

include <tunables/global>

/usr/share/org.gnome.Characters/org.gnome.Characters {
  include <abstractions/base>

  /usr/bin/gjs-console ix,
  /usr/share/org.gnome.Characters/org.gnome.Characters r,

}
```

Включаем режим комплейн

```
anastasya@ubuntu:~$ sudo aa-complain gnome-characters
Setting /usr/share/org.gnome.Characters/org.gnome.Characters to complain mode.
```

Проверяем работоспособность таблицы символов – работает!

```
anastasya@ubuntu:~$ gnome-characters
Gjs-Message: 10:03:18.083: JS LOG: Characters Application started
Gjs-Message: 10:03:18.351: JS LOG: Characters Application activated
```

Использую CENTOS 7

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра.
В SELinux используется модель Белла-Лападулы, это значит что пользователь с более низким уровнем доступа может читать и писать в файлы, которые создал сам и записывать информацию в файлы пользователя более высокого уровня доступа. В то же время пользователь с высшим уровшем доступа может читать/писать во все свои файлы и читать файлы пользователя более низкого уровня.

Проверила, что SELinux выполняется

```
[anastasya@localhost ~]$ getenforce
Enforcing
```

Более подробная информация о SELinux через утилиту

```
[anastasya@localhost ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
[anastasya@localhost ~]$ _
```

Установим нужные пакеты через команду yum install selinux-policy-mls
Посмотрим файл /etc/selinux/mls/setrans.conf

```
#
# Objects can be labeled with one of 16 levels and be categorized with 0-1023
# categories defined by the admin.
# Objects can be in more than one category at a time.
# Users can modify this table to translate the MLS labels for different purpose.
#
# Assumptions: using below MLS labels.
#  SystemLow
#  SystemHigh
#  Unclassified
#  Secret with compartments A and B.
#
# SystemLow and SystemHigh
s0=SystemLow
s15:c0.c1023=SystemHigh
s0-s15:c0.c1023=SystemLow-SystemHigh

# Unclassified level
s1=Unclassified

# Secret level with compartments
s2=Secret
s2:c0=A
s2:c1=B

# ranges for Unclassified
s0-s1=SystemLow-Unclassified
s1-s2=Unclassified-Secret
s1-s15:c0.c1023=Unclassified-SystemHigh

# ranges for Secret with compartments
s0-s2=SystemLow-Secret
s0-s2:c0=SystemLow-Secret:A
s0-s2:c1=SystemLow-Secret:B
s0-s2:c0,c1=SystemLow-Secret:AB
s1-s2:c0=Unclassified-Secret:A
s1-s2:c1=Unclassified-Secret:B
s1-s2:c0,c1=Unclassified-Secret:AB
s2-s2:c0=Secret-Secret:A
s2-s2:c1=Secret-Secret:B
s2-s2:c0,c1=Secret-Secret:AB
s2-s15:c0.c1023=Secret-SystemHigh
s2:c0-s2:c0,c1=Secret:A-Secret:AB
s2:c0-s15:c0.c1023=Secret:A-SystemHigh
s2:c1-s2:c0,c1=Secret:B-Secret:AB
s2:c1-s15:c0.c1023=Secret:B-SystemHigh
s2:c0,c1-s15:c0.c1023=Secret:AB-SystemHigh
```

Смотрим режим работы SELinux через конфигурационный файл командой командой /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Через редактор vim в файле /etc/selinux/config устанавливаем SELINUX = permissive и SELINUXTYPE = mls

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=mls
```

Проверим статус SELinux

```
[anastasya@localhost ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             mls
Current mode:                   enforcing
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
```

Для тестирования создаем двух новых пользователей First, Second и задаем им пароли.

```
[anastasya@localhost ~]$ sudo userdel First
[anastasya@localhost ~]$ sudo useradd -Z user_u First
[anastasya@localhost ~]$ sudo passwd First
Changing password for user First.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
```

```
[anastasya@localhost ~]$ sudo useradd -Z user_u Second
[sudo] password for anastasya:
[anastasya@localhost ~]$ sudo passwd Second
Changing password for user Second.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
```

Создаем текстовый файл от первого пользователя

```
[anastasya@localhost ~]$ su First
Password:
[First@localhost anastasya]$ cd
[First@localhost ~]$ touch text.txt
[First@localhost ~]$ ls
text.txt
[First@localhost ~]$ echo Hello_First_user > text.txt
[First@localhost ~]$ cat text.txt
Hello_First_user
```

Делаем тоже самое для второго. Он может прочитать свой файл, а другого пользователя - нет

Пытаюсь прочитать файл второго пользователя от имени первого – отказ в доступе

Можно сделать вывод о том, что все работает корректно. Работа в двухуровневой модели была продемонстрирована на скринах.