Практическое задание № 12.
Песочницы

Опубликовано **29.11.2022**

Дедлайн **13.12.2022**

1 Введение

Лабораторная работа посвящена настройке AppArmor. Работа рассчитана на выполнение с использованием Linux-систем на базе Debian. Проверена на Ubuntu.

Профили AppArmor хранятся в папке /etc/apparmor.d/. Профили описывают какие возможности программе разрешены, а какие – нет. AppArmor имеет два режима работы – complain и enforce. В первом режиме производится логирование нарушений политики, во втором – запрещается доступ.

Для генерации профиля и его обновления используется команда aa-genprof, которая позволяет пользователю выбрать какие действия следует разрешить или запретить программе.

1.1 Установка

```
sudo apt install apparmor apparmor-easyprof apparmor-profiles
sudo apt install apparmor-notify apparmor-profiles-extra apparmor-utils
```

1.2 Справка по командам

Просмотр статуса политики AppArmor и профилей.

```
sudo apparmor_status
```

Генерация или обновление профиля для приложения.

```
sudo aa-genprof executable
```

Перевод профиля в режим enforce.

```
sudo aa-enforce /path/to/profile
```

Перевод профиля в режим complain.

```
sudo aa-complain /path/to/profile
```

Отключение профиля. При этом включение осуществляется командами aa-enforce, aa-complain.

```
sudo aa-disable /path/to/profile
```

Перезагрузка профилей AppArmor.

```
sudo systemctl reload apparmor.service
```

2 Задания

2.1 Ограничение урона от уязвимостей

Выбрать сервис/программу с уязвимостью и рабочим эксплойтом. С помощью AppArmor сделать этот эксплойт неработоспособным (или ограничить его урон). При этом сама программа должна оставаться работоспособной. Заметим, что база `www.exploit-db.com` помимо эксплойтов содержит в себе также уязвимые сборки программ.

Примеры уязвимых программ:

1. Tiny HTTPd (такой сервер встречается на роутерах)
2. Уязвимая версия сервера Apache (CVE-2021-41773) из Задания №3.

Материалы

1. "Безопасный Linux. Часть первая. AppArmor – песочница для приложений"
   `https://www.ibm.com/developerworks/ru/library/l-apparmor-1/`
2. "Безопасный Linux. Часть вторая. AppArmor – разработка профилей"
   `https://www.ibm.com/developerworks/ru/library/l-apparmor-2/`
3. Tiny HTTPd 0.1.0 - Directory Traversal
   `https://www.exploit-db.com/exploits/42790/`