

Основы построения защищенных компьютерных сетей

Лекция 12
Песочницы

Семён Новосёлов

2022



Введение

Песочница — механизм изоляции приложений

- позволяет минимизировать урон от уязвимостей (включая 0-day) и эксплойтов к ним

Примеры:

- виртуализация
- UAC в Windows
- изоляция на основе правил (SELinux, AppArmor)



AppArmor

- модуль безопасности ядра Linux
- входит в стандартную поставку Ubuntu/Debian
- позволяет ограничивать программам различные действия
- например: запуск программ, доступ к сети, доступ к файлам

Установка Apparmor

Для Ubuntu:

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

Просмотр статуса:

```
sudo apparmor_status
```

Профили Apparmor

Описывают какие возможности программе разрешены, а какие – нет.

- хранятся в папке `/etc/apparmor.d/`
- их можно генерировать с помощью команды `aa-genprof`
- либо писать вручную с помощью специального языка

Режимы работы

AppArmor имеет два режима работы:

complain: логирование нарушений



```
sudo aa-complain profile_path
```

enforce: запрещается доступ



```
sudo aa-enforce profile_path
```

Генерация профиля

1. Запуск отслеживания событий для программы `executable`:
`sudo aa-genprof executable`
2. Запуск приложения
`executable`
3. Выполнение легитимных функций в приложении
4. Сканирование событий и выбор реакции (Запретить/Разрешить/...)
5. Завершение работы
(все остальные действия будут блокироваться)
6. Доработка профиля вручную
7. Можно запустить ещё раз для обновления
(если появились новые события в логе AppArmor)

Пример. Защита от инъекций команд ОС

Уязвимый код на PHP:

```
<?php
if(isset($domain) && $domain != "") {
    $output=null;
    exec("whois $domain", $output);
    foreach($output as $s){
        echo trim($s) . "<br/>";
    }
}
?>
```

Если запускать код на связке Nginx + php-fpm, то в профиле для php-fpm необходимо разрешить запуск whois и все зависимости

Правила

```
/usr/bin/dash cx,  
  
profile /usr/bin/dash {  
    network,  
    /usr/bin/dash mr,  
    /usr/bin/whois rix,  
    /dev/null rw,  
    /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2 mr,  
    /usr/lib/x86_64-linux-gnu/libc.so.6 mr,  
    /etc/ld.so.cache mr,  
    /usr/lib/x86_64-linux-gnu/libidn2.so.* mr,  
    /usr/lib/x86_64-linux-gnu/libunistring.so.* mr,  
    /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache mr,  
    /usr/lib/x86_64-linux-gnu/gconv/gconv-modules mr,  
    /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.d/ mr,  
    /usr/lib/x86_64-linux-gnu/libnss_mdns4_minimal.so.* mr,  
    /etc/services r,  
    /run/systemd/resolve/stub-resolv.conf r,  
    /etc/hosts r,  
    /etc/host.conf r,  
    /etc/nsswitch.conf r,  
    /run/php/php*-fpm.sock r,  
}
```

Литература и ссылки

- <https://apparmor.net/>
- <https://gitlab.com/apparmor/apparmor/-/wikis/QuickProfileLanguage>
- <https://manpages.ubuntu.com/manpages/jammy/en/man5/apparmor.d.5.html>

