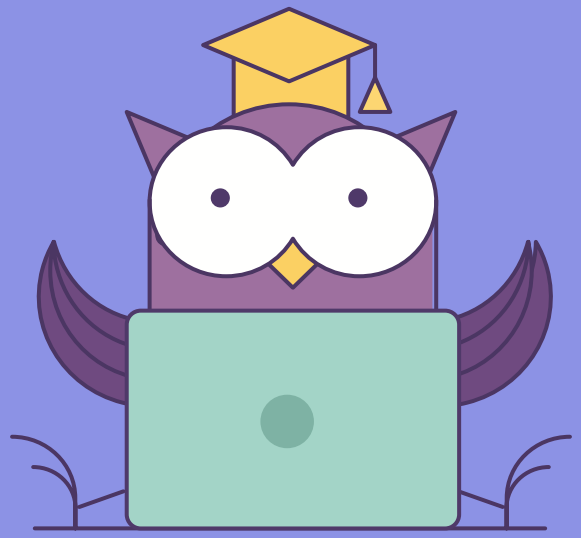
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Структура операционной системы Linux
Часть 2

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

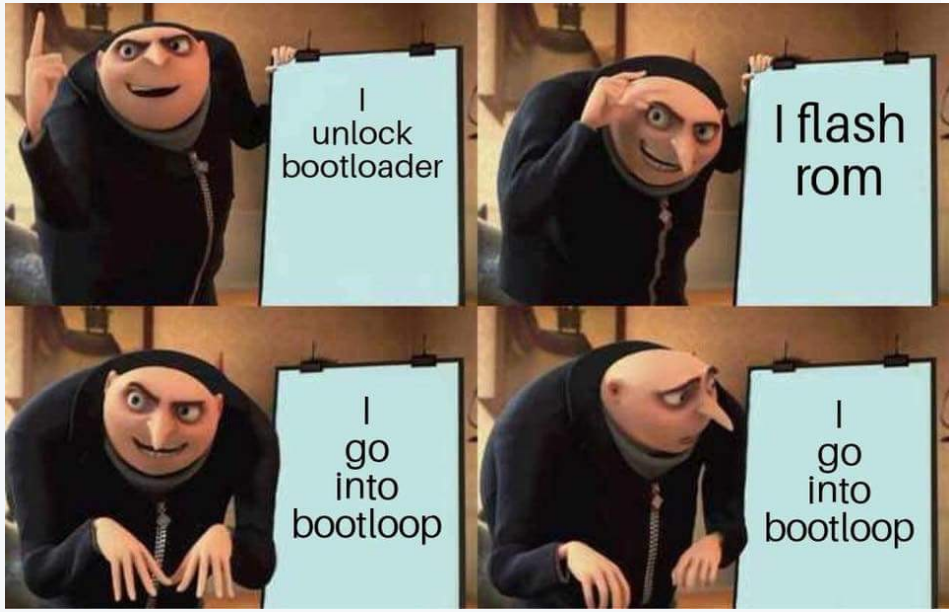
Содержание

- Что такое процесс
- Что такое демон
- Запуск процессов в операционной системе
- Разграничение доступа
- Мини-практика (http://ringzer0ctf.com/)

Цель занятия

1. Исследование классификации атак для операционной системы Linux

2. Использовать полученные данные для разбора атак на операционную систему



01

Что такое процесс

Linux процесс

Вторая по важности абстракция ядра

Что содержит в себе:

- Исполняемый код загруженного образа в память
- Описание всех используемых
- Информация об открытых файлах
- Информация об открытых сетевых соединениях
- Информация о выполняемых действиях (контексты потоков)

Linux процесс

Что важно знать

Какие характеристики процесса существуют:

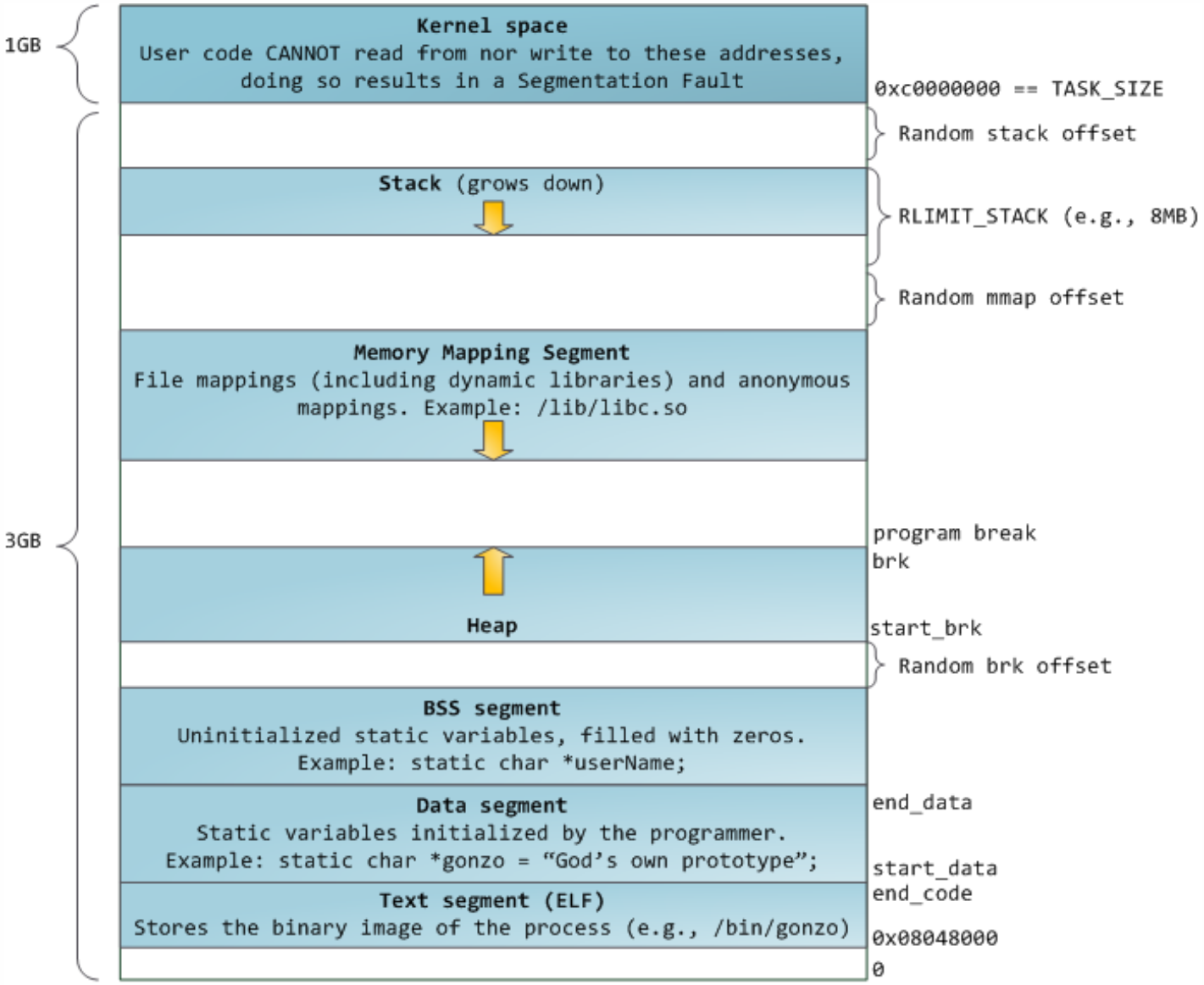
- Идентификатор процесса
- Имя процесса
- Путь до домашней директории файла
- Права Запуска

- Как посмотреть информацию?
- **ps**

00

Просмотр информации о процессах

Карта памяти процесса



02

Что такое демон

Демон

Процессы, которые запускаются системой

Для чего обычно используются:

- Файловые серевера
- Web Сервера
- Управление оборудованием
- Виртуализация
- Файловые системы

Как посмотреть состояние:

services

Systemctl

03

Запуск процессов в операционной системе

Особенности запуска процессов

Последовательность действий:

- Загрузка образа в память
- Запуск процесса

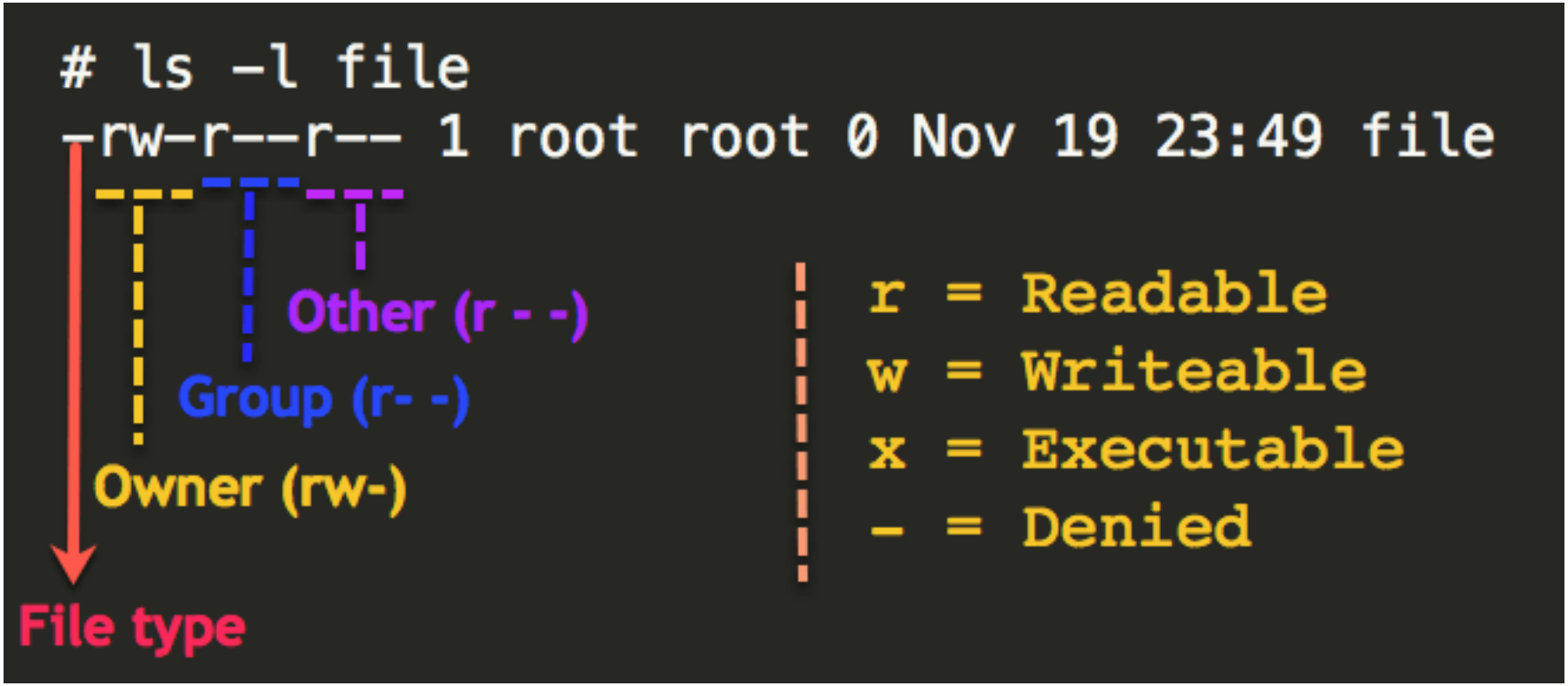
Какие системные вызовы используются:

- fork
- Exec

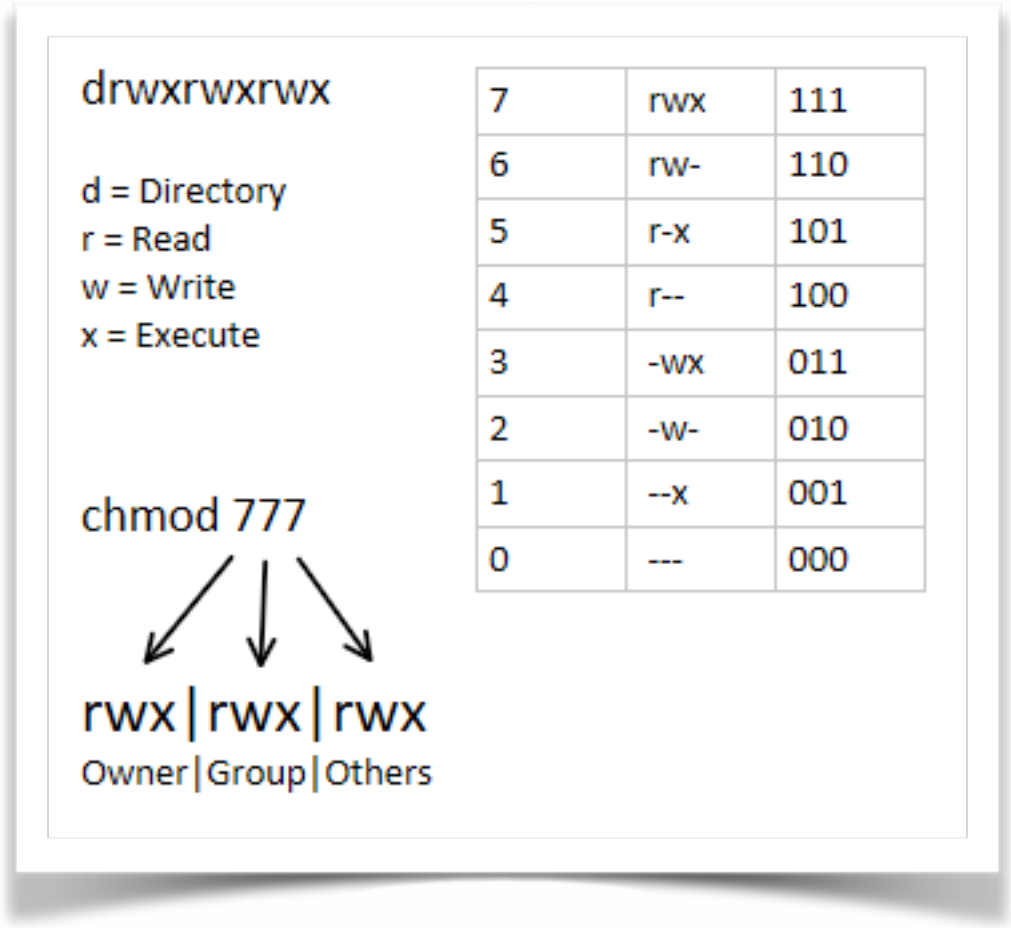
04

Разграничение доступа

Права доступа в файловой системе



Права доступа в файловой системе



7	rwx	111
6	rw-	110
5	r-x	101
4	r--	100
3	-wx	011
2	-w-	010
1	--x	001
0	---	000

Список исользуемых команд

- netstat - утилита для просмотра активных соединений
- ps - утилита для получения информации о запущенных процессах
- cat - утилита для редиректа потока данных
- grep - утилита для фильтрации вывода
- file - утилита для получения информации о формате файла
- mysql cli - консоль управления Mysql

Александр Колесников

Спасибо
за внимание!