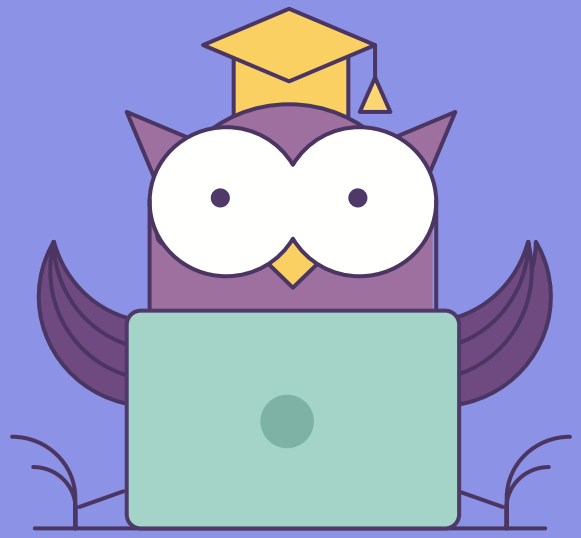
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Структура операционной системы Linux
Часть 3

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

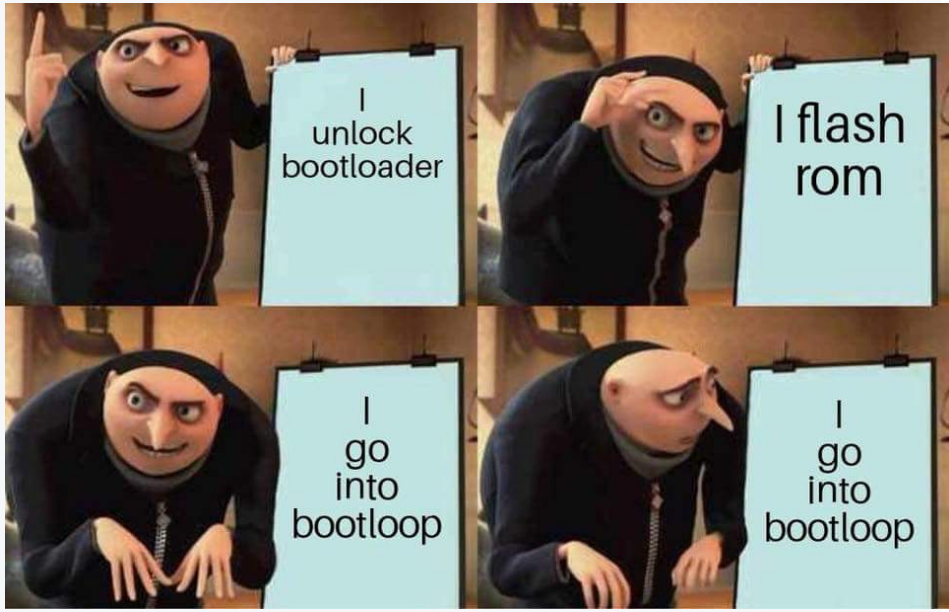
Содержание

- 100500 способов запустить bash (sh)
- Разбор заданий ringzer0team
- Уязвимости из заданий
- Где еще взять практику

Цель занятия

1. Исследование классификации атак для операционной системы Linux

2. Использовать полученные данные для разбора атак на операционную систему



01

100500 способов запустить bash (sh)

Примеры команд

- tar -cf /dev/null /dev/null --checkpoint=1 —checkpoint-action=exec=/bin/sh
- awk 'BEGIN {system(«/bin/sh")}'
- less /etc/profile; !/bin/sh
- vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh»)'
- gdb -nx -ex '!sh' -ex quit
- find . -exec /bin/sh \; -quit

02

Разбор заданий ringzer0team

03

Уязвимости из заданий

SQL Injection

- Класс атак на данные, который позволяет получать данные из реляционных баз данных.
- Причины возникновения - не верный процессинг данных, вводимых пользователями.
- Встречается в 90% случаев в Web-приложениях
- Элементарная проверка - поставить ‘ в поле ввода
- Популярное приложение для тестирования атаки - sqlmap

Local File Inclusion

- Класс уязимостей, который через функции web-приложения или через функции технологий, которые используются для его работы позволяет считывать файлы из файловой системы сервера

- Полезные символы и команды:
  - .
  - ..
  - /
  - http://target_ip/?page=php://filter/convert.base64-encode/resource=

Александр Колесников

Спасибо
за внимание!