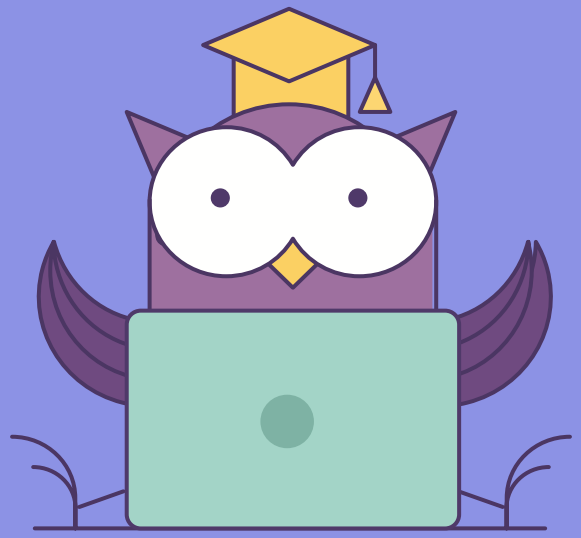

ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

# Особенности атак на операционную систему Linux

Колесников Александр Александрович

# Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

# Содержание

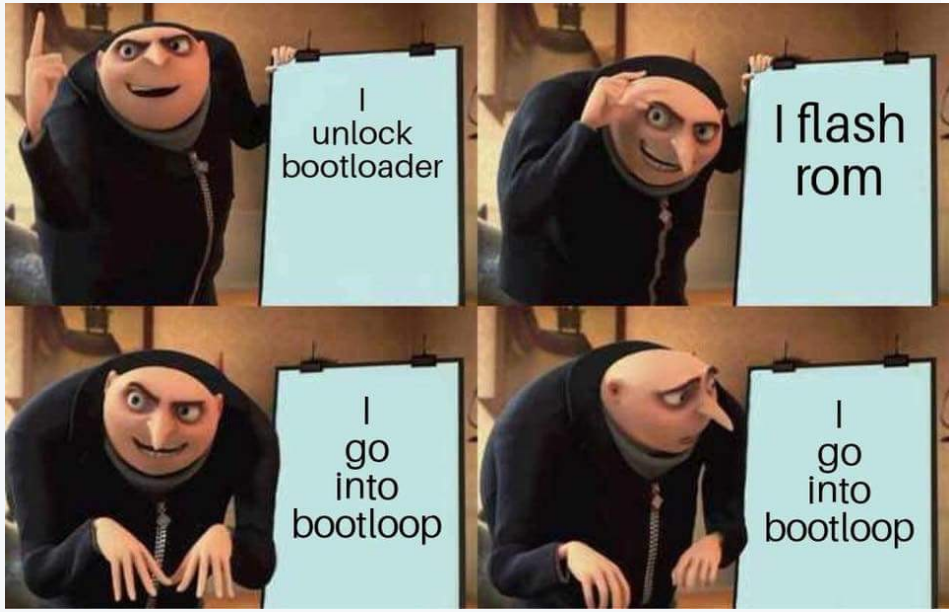
- Linux общие сведенья
- Классификация атак на Linux
  - Сетевые
  - Локальные

- Практическое задание:
  - Эксплуатация уязвимости в веб-приложении
  - Повышение приведений

# Цель занятия

1. Исследование классификации атак для операционной системы Linux

2. Проведение отдельных атак в лабораторных работах



01

# Операционная система Linux

# Linux

Операционная система, которая, по сути не имеет общего облика и публикуется в виде ядра.

Была создана в 1991 году.

Особенности:

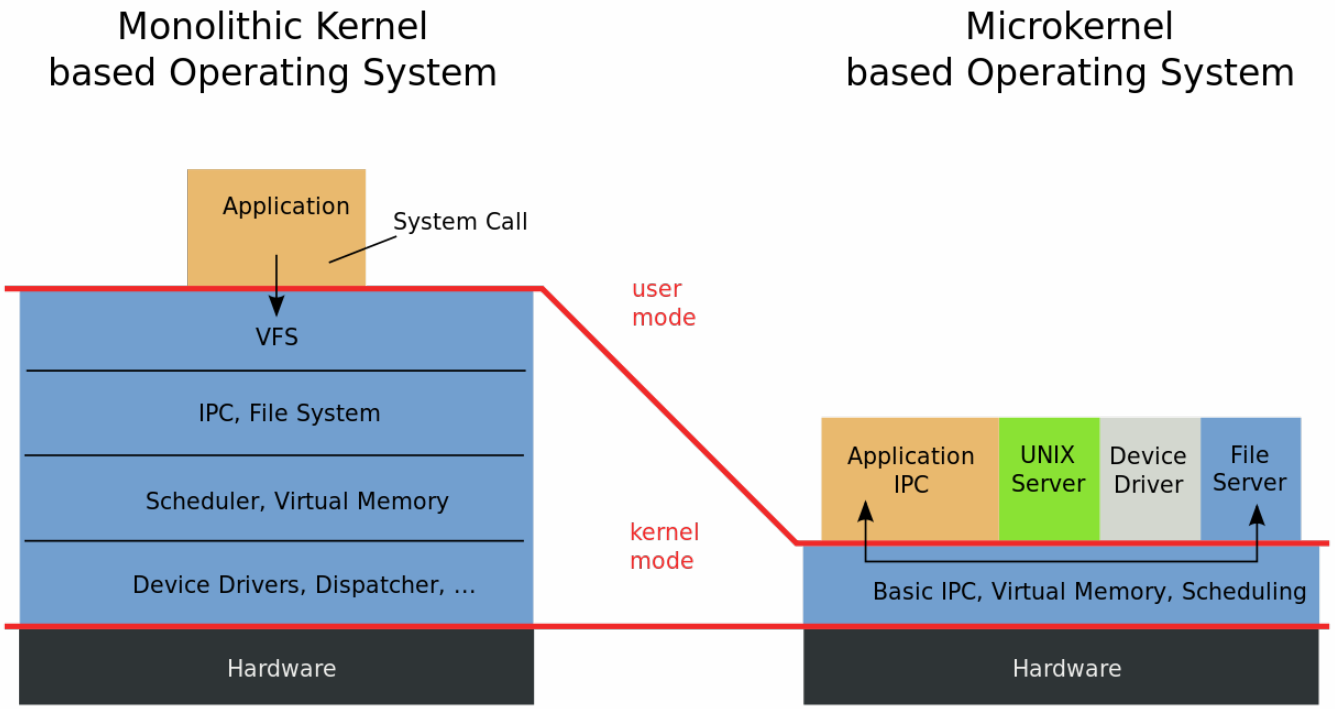
- Открытый исходный код
- Собственна архитектура ядра
- Ориентирована на программистов
- Ориентирована на использование на серверах (хотя в последние годы и старается распространиться на обычные ПК)

# Коренное отличие

Операционная система построена на собственной концепции.

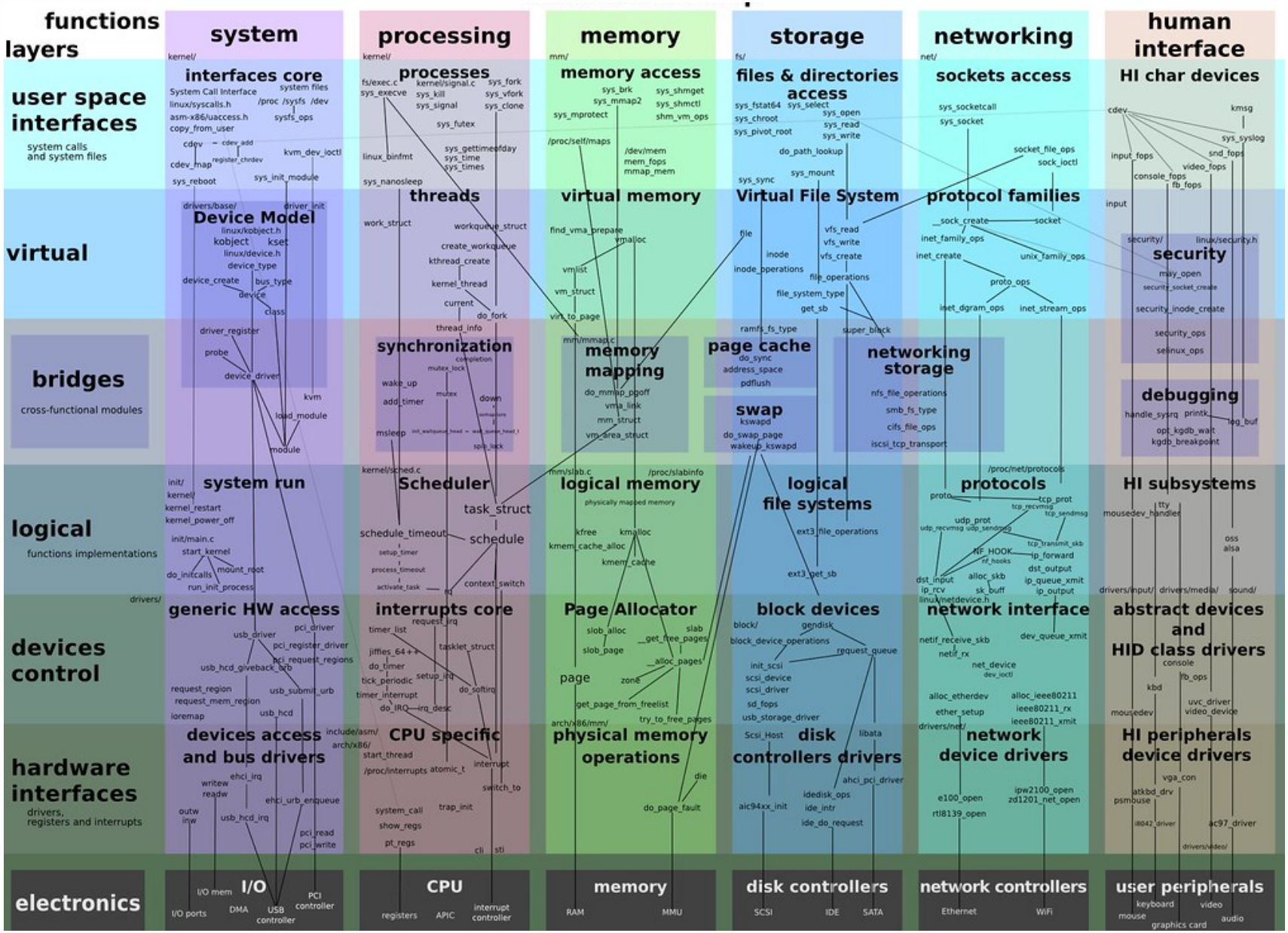
Четкое разграничение на код ядра и пользовательского пространства.

Встроенные механизм разграничения доступа



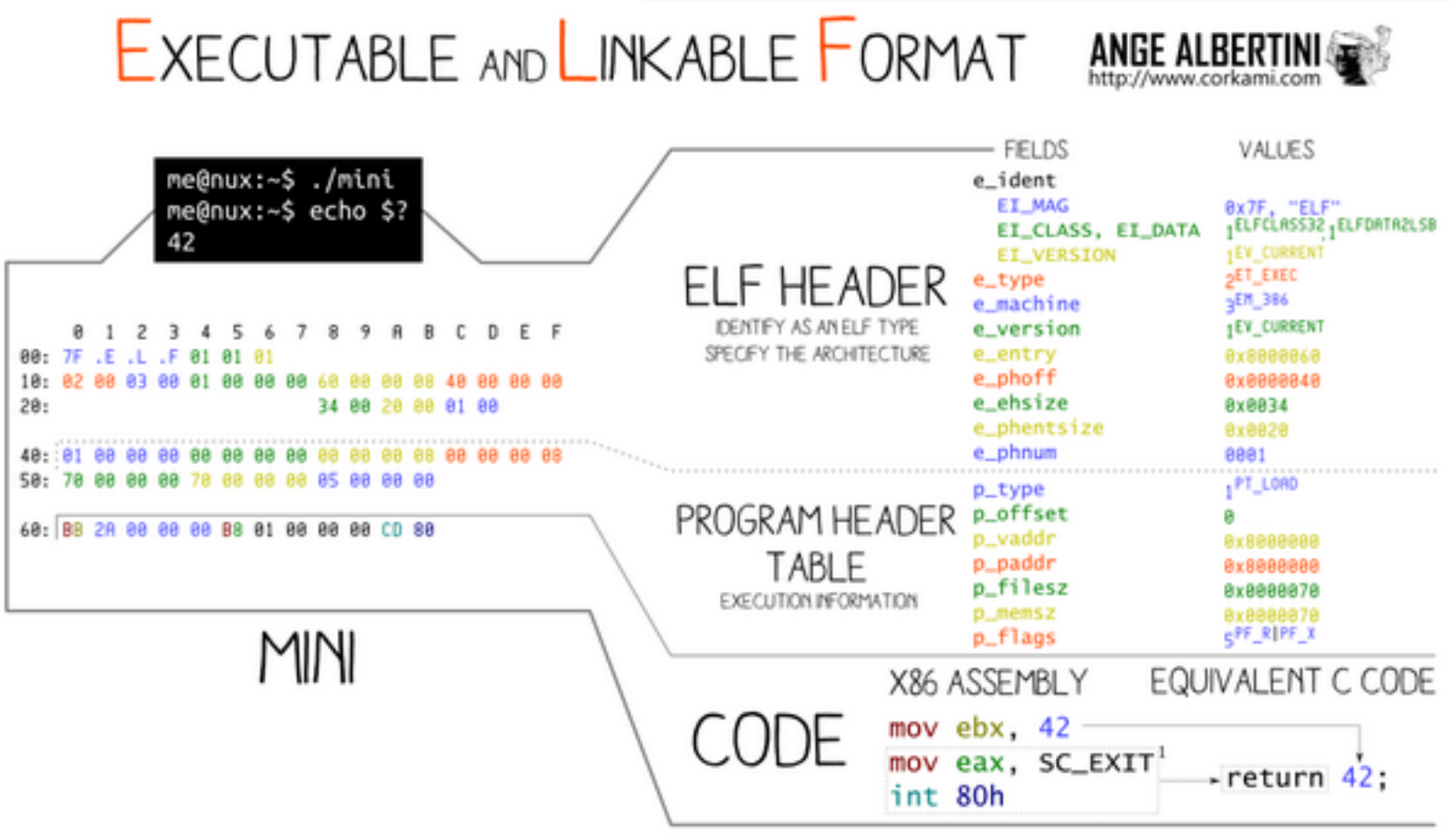
# Подробный вид составных блоков

http://www.makelinux.net/kernel_map/



# Исполняемый файл

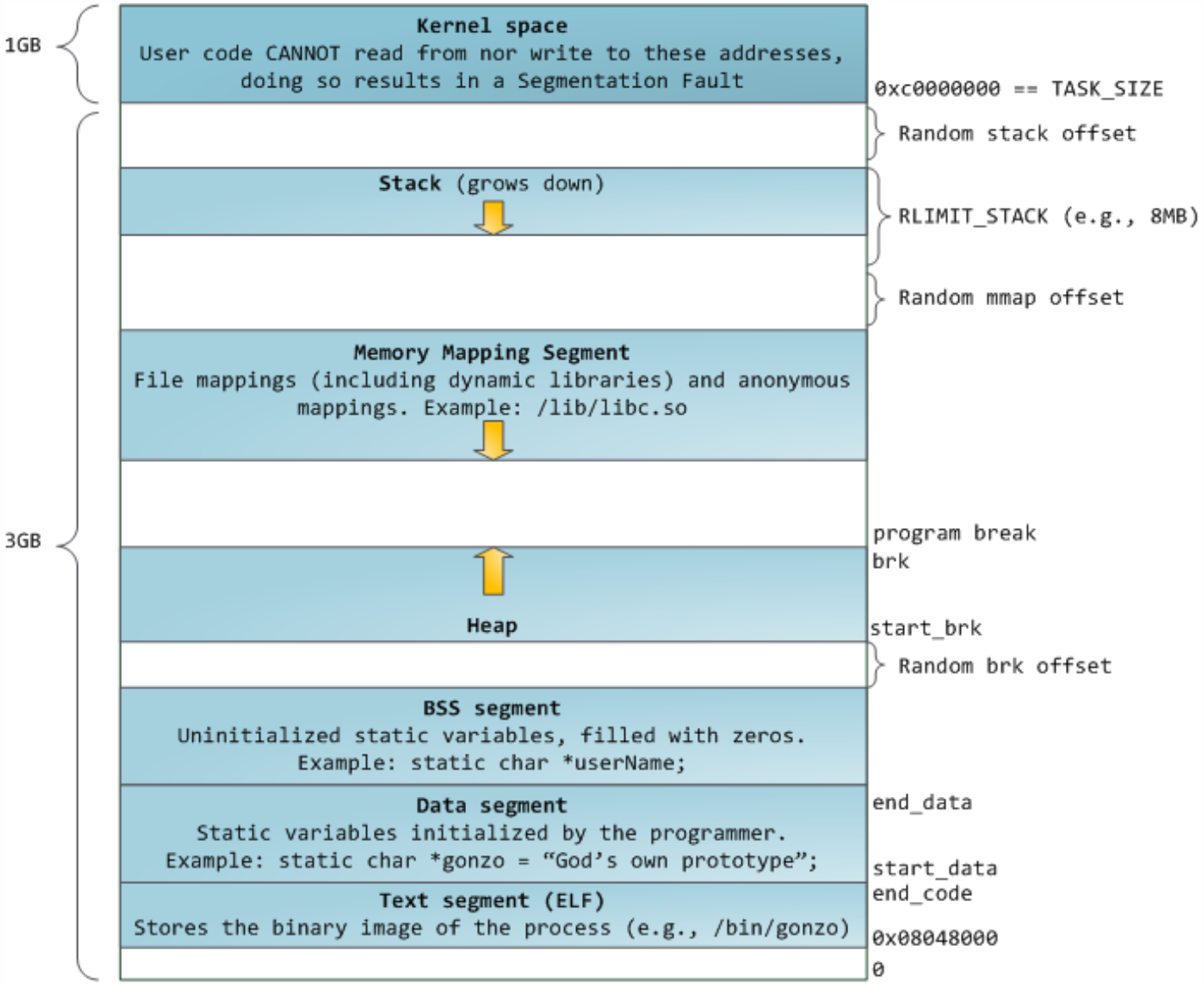
Операционная система использует тип файла



00

# Просмотр формата файла

# Карта памяти процесса



# Настройка GEF

Для корректной работы GEF необходимо предустановить pip3:

- apt-get install python3-pip
- wget -q -O- https://github.com/hugsy/gef/raw/master/scripts/gef.sh | sh

01

# Отладка в операционной системе Linux

# Основные типы уязвимостей

Типы уязвимостей очень похожи на те, что были в Windows:

- Type confusion
- Buffer overflows on stack/heap
- Race Conditions
- UAFs
- Integer overflow/underflow

02

# Локальные атаки на Linux

# Локальные атаки

Основная цель атак - получение прав привилегированного пользователя - root

Существуют следующие подходы:

- Эксплуатация уязвимостей ОС
- Process Injection
- Setuid и Setgid
- Sudo Caching
- Sudo
- Использование данных аккаунтов
- WebShell

# Эксплуатация уязвимости ОС

Использование особенности или недостатка стандартного механизма, который работает в системе Linux.

Примеры таких эксплойтов:

- Dirty Cow (CVE-2016-5195) - эксплойт, который до сегодняшнего дня применим для повышения привелегий вплоть до версии ядра 3.9.

# Process injection

Использование механизмов операционной системы, которые предоставляют возможность подгрузки дополнительных модулей в адресное пространство любого приложения.

Для linux это:

- **LD_PRELOAD**, **LD_LIBRARY_PATH** - переменные окружения, которые позволяют указать откуда загружать модули в работающий процесс
- **Trace system calls** - используется для того чтобы модифицировать работу приложения на-лету
- **/proc/[pid]/mem** - предоставляет доступ к памяти процесса и, если хватает прав, позволяет модифицировать его
- **VDSO hijacking** - техника, которая позволяет заменить системный вызов и выполнить свой код без записи его в защищенные участки памяти процессов

# GetUID и SetGID

Механизм разграничения доступа, который позволяет назначить приложению права, которых нет у пользователя.

Например:

- Приложение передает данные по сети, ей необходимо открыть порт
  - Так как у обычного пользователя нет прав на открытие порта, то приложение может быть наделено такими правами через uid или gid более привилегированного пользователя в системе или группы
- Назначение на практике выглядит так:
  - chmod u+s filename
  - chmod 4777 filename

# Sudo Caching

Утилита Sudo может использовать кэширование для того чтобы администратор больше не вводил пароль для выполнения команды.

Суть механизма:

- После ввода пароля для выполнения команды, в sudo может быть активирован timestamp_timeout
- Для проверки оставшегося времени sudo обращается к файлу: /var/db/sudo чтобы посмотреть когда последний раз осуществлялся к нему доступ
- Полученное значение е сравнивается с tty_tickets, которые генерируются для каждого пользователя и так же имеют тайм-аут

# Sudo

Операционная система предоставляет механизмы для разграничения доступа, которые используют файл /etc/sudoers - он описывает:

- Какие пользователи могут выполнять какие команды
- Так же можно определить какие группы будут иметь какой доступ к ресурсам в системе и какие команды выполнять
- Файл так же может определить должен ли пользователь вводить пароль для выполнения команд, на которые введены ограничения

# Использование аккаунтов и Web Shell

Две самые относительно простые атаки, которые могут быть выполнены как играючи так и очень продумано.

Реализация использование аккаунтов:

- Хищение учетных данных пользователей и использование их в процессе проведения атаки
- Фишинг
- ВПО

Реализация web shell:

- Использование уязвимости в веб-приложении
- Использование лазейки в конфигурации веб-приложения

03

# Сетевые атаки на Linux

# Сетевые атаки

Подвержены внутренности ядра, которые работают с обработкой пакетов.

Так же, могут быть проэксплуатированы приложения, которые работают по сети.

Что может произойти при удачной атаке:

- Получение привелигированного доступа к системе
- DDoS

00

# Практика сетевых и локальных атак

# Список исользуемых приложений

- nmap - сканер, используется для определения конфигурации хоста
- enum4linux - утилита для получения информации о smb общих ресурсах
- Smbclient - клиент для использования smb
- Metasploit - фреймворк дя автоматизации pentest
- mysql cli - консоль управления Mysql

# Александр Колесников

# Спасибо
# за внимание!