Исследование процесса, бэкдоры

Сабина Жигальская
Специалист по комплексной защите информации

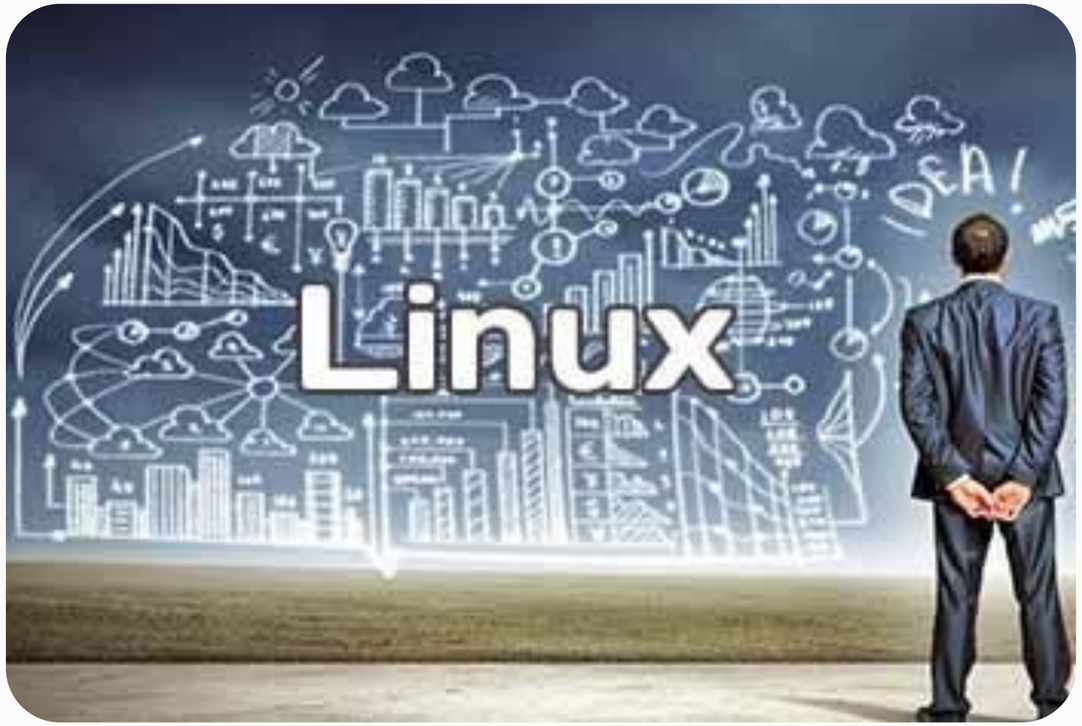
Skillbox

Цели урока

- Вспомним, что такое процесс
- Рассмотрим утилиты исследования процесса
- Узнаем, что такое бэкдор

Процесс

Процесс — это выполняющаяся программа в Linux. Каждый процесс имеет уникальный идентификатор процесса, PID.



Исследование процессов

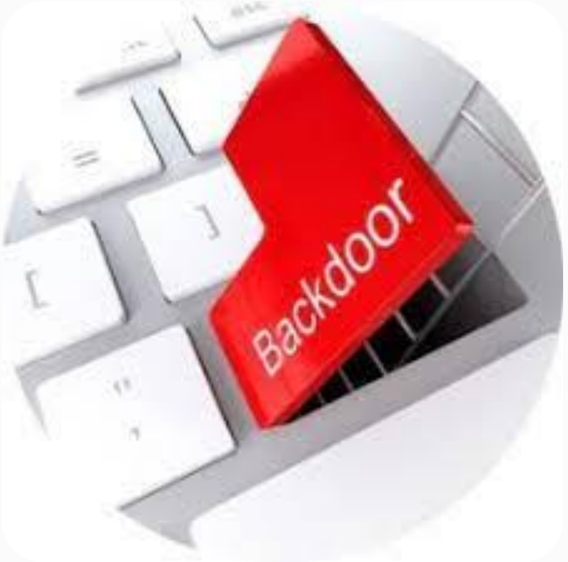
Основной инструмент для исследования процессов — утилита **PS**. Она выводит состояние процессов в системе.

Утилита **W** демонстрирует список всех вошедших в сеанс пользователей и запущенные ими задания.

Бэкдор

В системе могут быть не только легальные процессы.

Бэкдор является вредоносной программой, которая используется злоумышленниками для получения несанкционированного удалённого доступа к компьютерной системе за счёт уязвимости в системе безопасности.



Бэкдор

Большинство бэкдоров должны как-то проникнуть в компьютер, но некоторые из них не требуют установки, так как их части **уже интегрированы** в программное обеспечение, которое работает на удалённом хосте.

Распространение бэкдоров

Основные способы попадания в систему:

- случайно установиться на компьютер пользователем
- установиться другими паразитами: вирусами, троянами или шпионскими программами
- интегрироваться в конкретные приложения
- использовать определённые уязвимости программного обеспечения

Известные бэкдоры

- **FinSpy** позволяет удалённому злоумышленнику загрузить и запустить любой файл из интернета
- **Tixanbot** даёт полный доступ к заражённому компьютеру. Этот бэкдор чрезвычайно опасен
- **Briba** предоставляет удалённый и несанкционированный доступ к заражённой компьютерной системе

Выводы урока

- Кроме легальных процессов есть и не совсем «хорошие». Они называются бэкдоры
- Есть разные способы проникновения бэкдоров в систему: при участии пользователя или других программ
- Примеры распространённых бэкдоров: Briba, Tixanbot, FinSpy