Защита SSH

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цель урока

Узнать, как защититься от несанкционированного доступа по SSH.

SSH

Синтаксис команды выглядит следующим образом:

$ ssh [опции] имя пользователя@сервер [команда]

ОПЦИИ:

- f — перевести ssh в фоновый режим
- g — разрешить удалённым машинам обращаться к локальным портам
- l — имя пользователя в системе
- n — перенаправить стандартный вывод в /dev/null
- p — порт ssh на удалённой машине
- q — не показывать сообщения об ошибках
- v — режим отладки
- x — отключить перенаправление X11
- X — включить перенаправление X11
- C — включить сжатие

Способы защиты. Фаервол

Первый способ — это защита средствами фаервола.

Данный способ защиты не всегда и не всем подходит, но всё же остаётся действенным для отражения атак с неизвестных ip-адресов.

В настройках фаервола указываются правила доступа к ssh-серверу с нужных адресов и запрещающее правило для остальных.

Способы защиты. Пароль

Самый стандартный способ — это авторизация по паролю. После установки ssh-сервер висит на 22 порту.

Пароль должен быть СЛОЖНЫМ!

Способы защиты. Порт

Также помогает поменять стандартный порт размещения SSH.

Стандартный порт — 22. Поменять порт можно в конфигурационном файле.

Способы защиты. Доступ по ключам

Принцип работы:

На компьютере пользователя создаётся пара: приватный ключ и публичный ключ.

Приватный ключ пользователь хранит у себя — это его зона ответственности, а публичный передаётся на сервер.

Для увеличения безопасности пользователь может установить пароль на приватный ключ.

Вывод урока

Существует много различных способов защиты ssh. Комбинируя их между собой, можно значительно повысить уровень защиты сервера.

Выводы модуля

- В этом модуле мы обсудили, как работать с учётными записями, а именно — как создавать. Также научились работать с групповыми учётными записями и списками контроля доступов
- С точки зрения кибербезопасности мы узнали, как пользователи могут подключаться к компьютерам по удалённому доступу — с помощью SSH
- Разобрали, что SSH тоже надо защищать, и обсудили способы защиты