

SSH

Сабина Жигальская

Специалист по комплексной защите информации

Skillbox

Цели урока

- ✓ Узнать, что такое SSH
- ✓ Понять особенности SSH

SSH

SSH

SSH — Secure Shell — это протокол удалённого управления компьютером с операционной системой Linux.

Особенности SSH

Основные преимущества SSH-протокола:

- возможность работать удалённо на компьютере через командную оболочку
- алгоритмы, обеспечивающие надёжное шифрование
- SSH — универсальное решение, которое даёт возможность передачи любого протокола
- сжатие данных для их дальнейшего надёжного шифрования и передачи
- защита канала передачи от возможных сторонних подключений с последующим перехватом данных

SSH клиент-сервер

Принцип работы SSH заключается в том, что SSH-сервер принимает соединение от машины пользователя и производит аутентификацию. Она может быть осуществлена 3 способами:

- по IP
- по публичному ключу клиента
- по зашифрованному паролю клиента

Защита SSH

- Запрещение удалённого root-доступа по паролю
- Запрещение подключения с пустым паролем или отключение входа по паролю (использование ключей)
- Выбор нестандартного порта для SSH-сервера (стандартный — 22)
- Использование длинных SSH2 RSA-ключей (2048 бит и более) для аутентификации
- Ограничение списка IP-адресов, с которых разрешён доступ (например, блокированием порта на уровне файервола)
- Отказ от использования распространённых или широко известных системных логинов для доступа ПО

Вывод урока

Протокол SSH имеет надёжную защиту, поэтому часто используется системными администраторами для удалённого управления компьютером.