УРОК 5. SSH - SECURED SHELL

ЧТО ТАКОЕ SSH

SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. SSH, или Secure Shell, представляет собой протокол для безопасной удаленной работы с компьютерами и передачи данных через незащищенную сеть. Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. Этот протокол обеспечивает шифрование данных и аутентификацию, что делает его надежным средством для удаленного доступа и управления удаленными системами.

Простым языком - ssh помогает нам подключаться к удаленным системам, компьютерам и серверам и шифровать наши данные при подключении.

Характеристики SSH:

Шифрование данных: Весь трафик между клиентом и сервером шифруется, предотвращая перехват и прослушивание данных третьими лицами.

Аутентификация: SSH использует различные методы аутентификации, такие как пароли, открытые и закрытые ключи, что делает процесс входа более безопасным и гибким.

Удаленный доступ: SSH позволяет пользователям входить в удаленные системы с помощью командной строки, предоставляя возможность выполнения команд и управления удаленными ресурсами.

Передача файлов: SSH также может использоваться для безопасной передачи файлов между компьютерами с использованием утилиты SCP (Secure Copy)

КЛЮЧ SSH

Генерация SSH-ключа включает в себя создание пары ключей: приватного и публичного.

Для генерации ключа нужно ввести определенные команды в командной оболочке.
Ввод команды ssh-keygen:

```
bitnami@ip-172-31-39-14:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/bitnami/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/bitnami/.ssh/id_rsa.
Your public key has been saved in /home/bitnami/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:LpIE32FeUL8IavLjeDSd2yWfQO1w7W+JYN90+SyJXyA bitnami@ip-172-31-39-14
The key's randomart image is:
+---[RSA 2048]----+
|      ...        |
|       . .       |
|  .   + ....     |
|   o = +o.o..    |
|  . =.ooS+..E . .|
|   =o.o.o = ...o.|
|   .=..o.* + * =o|
|   o.o... o + B.o|
|  ...        o.. |
+----[SHA256]-----+
```

Если мы укажем имя файла для сохранения ключа, то по умолчанию ключ будет сохранен в домашнем каталоге пользователя. Просто нажмите Enter, если вы хотите сохранить ключ по умолчанию в ~/.ssh/id_rsa и ~/.ssh/id_rsa.pub
Затем нас попросят установить пароль (по желанию). Это дополнительный уровень безопасности. Если не желаете устанавливать пароль, просто нажмите Enter.

Нужно нажать несколько раз на enter, чтобы создать ключ без дополнительного пароля с шифрованием и параметрами по умолчанию.

Рассмотрим публичные и приватный файлы ssh ключа:

Если мы использовали параметры по умолчанию, то файлы ключа буду находиться в скрытой папке .ssh в домашней папке пользователя, если вы указывали название для ключа, то находится он будет в той же папке, где происходила генерация этого ключа.

Для того, чтобы посмотреть эти файлы можем использовать команды:

- cat ~/.ssh/id_rsa.pub
- cat ~/.ssh/id_rsa

Приватный ключ будет сохранен в файле, который вы указали, либо ~/.ssh/id_rsa а публичный ключ — в файле с тем же именем, но с .pub в конце.

Пример публичного ключа:

```
bitnami@ip-172-31-39-14:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCuklpPh4bIgOqUgy8wa7QrNY9F0OQZI9S24Pk/OaE7tmYj
LtsCI62AIS9XcsbNAQyRKnsj8d6pCPAgM1deTDwhWwkO3KzufAdMDVEnqJltB7SHYRuUfIFye8ufrSytAGIx
byCTvokZmMBvoODW3tck1XMxWVWS1dV6tinMeZ2QR5DPkx0d8uXbzWz7 bitnami@ip-172-31-39-14
```

Через пробел указано:

- ssh-rsa: указывает на использование алгоритма RSA.
- AAAAB3NzaC1yc2EAAAADAQABAAABAQC9...: представляет собой саму публичную часть ключа, которая будет длинной в несколько сотен символов. Это уникальная строка, содержащая информацию о ключе.
- bitnami@ip-172-31-39-14: комментарий об авторе этого ключа, который был указан при создании ключа. Он не является обязательным и может быть отсутствовать.

В ОС под управлением Linux важен регистр и каждый пробел (пробел является символом и так же виден системой), поэтому при копировании ключа важно не захватить лишние символы.

Использование ssh ключа:

Рассмотрим аналогию с обычным замком и физическим ключом для лучшего понимания концепции публичного и приватного ключей.

Приватный ключ (это Физический ключ, кусок металла, это что-то, что вы храните в тайне и используете для открытия замка). Только вы обладаете этим ключом.

Публичный ключ (Замок на\ в двери)– это что-то, что вы распространяете и предоставляете другим для проверки вашей подлинности. Любой может подойти к двери и посмотреть на этот замок. МОжет даже попробовать его открыть своим ключом (что конечно же не получится).

Открытие замка (Аутентификация):
Пример с замком: Вы вставляете физический ключ в замок. Если форма ключа соответствует форме замка, замок открывается. Аналогично, при использовании SSH, ваш приватный ключ используется для аутентификации. Если публичный ключ который находится на сервере, а вы предоставляете приватный ключ удаленному серверу, происходит проверка, что оба ключа является частью сгенерированной пары приватного и публичного ключа на вашем компьютере. Если это - две половинки одного ssh ключа, то вам разрешен доступ.

ЗАДАНИЕ ДЛЯ ЗАКРЕПЛЕНИЯ

1. Зайти на учебный сервер.
2. Вывести публичный ключ и скопировать его.
3. При помощи cat выводим содержимое публичного ключа, если вы дали ему какое-то имя при генерации.
4. Отправить этот ключ в чат.
5. Преподаватель добавит этот ключ в специальный файл, где расположены все публичные ключи тех, кому разрешен доступ к серверу.
6. Зайти на сервер (установить ssh соединение).
7. Отправить в чат скриншот того, что вы увидели после входа.
8. Создать свою рабочую папку на сервере:
   Воспользоваться командой:
   mkdir /opt/ИМЯ_ВАШЕЙ_ГРУППЫ/ВАШЕ_ИМЯ

Вход на учебный сервер:

- Для windows в PowerShell: clip < ~/.ssh/id_ed25519.pub
- Для mac и Linux: Выводим публичный ключ и копируем его - cat ~/.ssh/id_rsa.pub
  Либо при помощи cat выводим содержимое публичного ключа, если вы дали ему какое-то имя при генерации. cat *.pub

Преподаватель добавит этот ключ в специальный файл, где расположены все публичные ключи тех, кому разрешен доступ к серверу.

Публичный ключ (id_rsa.pub) добавляется в файл ~/.ssh/authorized_keys на удаленном сервере, чтобы разрешить доступ.

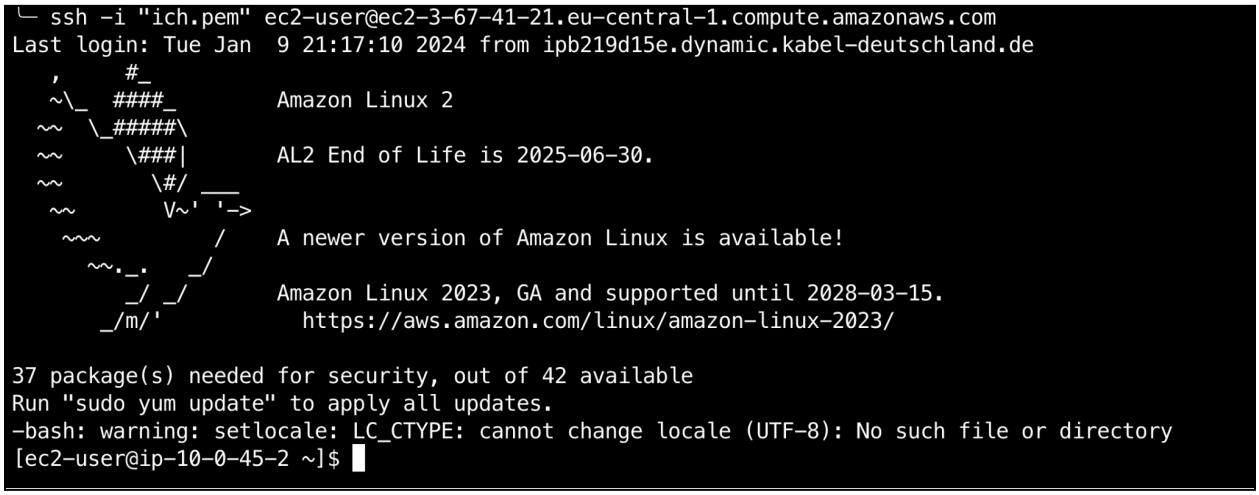
Для редактирования этого файла используем nano или другой текстовый редактор
nano .ssh/authorized_keys

Теперь пользователи, которым был предоставлен доступ, могут зайти на сервер (установить ssh соединение):

ssh -i ~/.ssh/id_rsa ec2-user@linux.itcareerhub.de

- ssh - мы запускаем ssh соединение для подключения к удаленному устройству;
- -i ~/.ssh/id_rsa - путь, по которому лежит наш приватный ключ на нашей машине
- ec2-user@linux.itcareerhub.de - непосредственный адрес нашего сервера. (иногда он выглядит как IP- адрес)
- ec2-user - это имя пользователя, под которым мы входим в систему.
- @ - разделитель

После входа мы видим приветствие и сразу попадаем в домашнюю папку нашего пользователя.



SCP

SCP (Secure Copy Protocol) - это протокол для безопасной передачи файлов между компьютерами по сети. Он предоставляет защищенную и шифрованную передачу данных, основанную на протоколе SSH (Secure Shell).

SCP позволяет копировать файлы между локальной и удаленной системами или между двумя удаленными системами

ЗАДАНИЕ ДЛЯ ЗАКРЕПЛЕНИЯ

1. Скопировать файл из сервера в текущую рабочую папку. Обращаем внимание на . в качестве точки назначения.
   scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2
2. Пример:
   scp -i ~/.ssh/id_rsa
   ec2-user@linux.itcareerhub.de:///opt/ИМЯ_ВАШЕЙ_ГРУППЫ/ВАШЕ_ИМЯ/file .