**федеральное государственное автономное образовательное учреждение высшего образования**



**МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**(ВЫСШАЯ ШКОЛА ПЕЧАТИ И МЕДИАИНДУСТРИИ)**

**(Факультет информационных технологий)**

***(Институт Принтмедиа и информационных технологий)***

***Кафедра Информатики и информационных технологий***

**направление подготовки**

**09.03.02 «Информационные системы и технологии»**

**ЛАБОРАТОРНАЯ РАБОТА № 7**

**Дисциплина:** Операционные системы

**Тема: Удаленный доступ по SSH**

**Выполнил: студент группы 231-338**

Шаура Илья Максимович

(Фамилия И.О.)

**Дата, подпись** 04.05.2024  ***\_\_\_\_\_\_\_\_\_\_\_***

(Дата) (Подпись)

**Проверил: *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_***

(Фамилия И.О., степень, звание) **(Оценка)**

**Дата, подпись** \_\_\_\_\_\_\_\_\_\_\_\_\_\_  ***\_\_\_\_\_\_\_\_\_\_\_***

(Дата) (Подпись)

**Замечания: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Москва**

**2024**

**Лабораторная работа № 7.**

1) Принцип работы SSH

**Что такое SSH?**

**SSH** — сокращение от «secure shell» (безопасная оболочка). Это протокол, который чаще всего используют для управления удалёнными компьютерами по сети.

**Как устанавливается сессия SSH?**

Есть несколько шагов, которые нужно пройти, чтобы начать SSH-сеанс между компьютерами.

1. Сначала нужно обеспечить безопасный способ обмена сообщениями между компьютерами, то есть настроить зашифрованный канал.
2. Далее нужно проверить целостность данных, отправляемых клиентом.
3. После этого проверяется подлинность клиента.

После этих трёх шагов мы можем безопасно общаться с удалённым компьютером, делиться секретными данными, а также проверить, есть ли у клиента разрешение на доступ к хосту. Каждый из разделов ниже будет более подробно описывать эти действия.

**Настройка зашифрованного канала**

Вся информация, отправляемая с использованием SSH, зашифрована. Обе стороны должны знать и понимать способ шифрования.

Для шифрования передаваемых данных используется симметричное шифрование. Суть данного подхода заключается в том, что оба компьютера имеют одинаковый ключ шифрования, который называется «симметричный ключ». Симметричное шифрование работает очень хорошо, но только до тех пор, пока сторонние не имеют доступа к ключу.

Один компьютер может создать ключ и отправить в виде сообщения через интернет. Но сообщение ещё не будет зашифровано, поэтому любой, кто перехватит его, сразу же сможет расшифровать все следующие сообщения.

Решение этой проблемы состоит в использовании протокола обмена ключами Диффи-Хеллмана. Оба компьютера создают свой закрытый и открытый ключ. Вместе они образуют пару ключей. Компьютеры делятся своими открытыми ключами друг с другом через интернет. Используя свой закрытый и чужой открытый ключ, стороны могут независимо сгенерировать одинаковый симметричный ключ.

**Верификация**

Следующий этап процесса установки сеанса SSH заключается в проверке того, что данные не были подделаны во время их передачи и что другой компьютер действительно является тем, за кого себя выдаёт.

Для верификации используют хеш-функцию. Это математическая функция, которая принимает входные данные и создаёт строку фиксированного размера.

Важной особенностью этой функции является то, что практически невозможно определить входные данные, зная лишь результат её работы.

После того как клиент и хост сгенерировали свои симметричные ключи, клиент использует хеш-функцию для генерации HMAC, что означает «код аутентификации сообщений, использующий хеширование». Клиент отправит этот HMAC на сервер для верификации.

Функция хеширования использует:

* симметричный ключ клиента,
* порядковый номер пакета,
* содержимое сообщения (зашифрованное).

Когда хост получает HMAC, он может использовать ту же самую хеш-функцию с этими тремя компонентами:

* собственный (идентичный клиентскому) симметричный ключ;
* порядковый номер пакета;
* зашифрованное сообщение.

Если сформированный хеш совпадает с HMAC, полученным от клиента, то мы можем быть уверены, что подключаемый компьютер — это компьютер с симметричным ключом, потому что только хост и клиент знают симметричный ключ, а другие компьютеры — нет.

Прелесть этого подхода в том, что мы не просто проверили личность клиента и убедились, что данные не были подделаны, но мы сделали это без передачи какой-либо секретной информации.

**Аутентификация**

Даже если мы используем симметричные ключи для безопасного общения, мы не знаем, имеет ли подключающийся компьютер разрешение на доступ к содержимому хоста. Для того чтобы проверить это, необходимо произвести аутентификацию.

Многие используют аутентификацию по паролю. Клиент отправляет хосту зашифрованное сообщение, содержащее пароль. Хост его расшифровывает и ищет пароль в базе данных, чтобы удостовериться, есть ли у клиента разрешение на доступ. Использование пароля для аутентификации допустимо, но имеет свои недостатки, так как необходимо хранить все пароли на сервере.

Более безопасной является аутентификация по сертификату. Сформировав сертификат, клиент единожды вводит пароль для доступа к серверу и отправляет ему открытую часть сертификата. В дальнейшем ввод пароля не требуется. Этот подход считается более безопасным, чем просто использование пароля, поскольку не подразумевает хранение секрета пользователя на хосте.

SSH — это важный инструмент, используемый для удалённого управления другими компьютерами. Он безопасен, поскольку оба компьютера могут шифровать и дешифровать сообщения с использованием симметричных ключей.

2) Установка SSH-сервера

Служба SSH позволяет получить доступ к терминалу удаленного компьютера и выполнить там все необходимые вам команды. При своей простоте она достаточно безопасна, чтобы использоваться для решения серьезных коммерческих задач, так и задач обычных пользователей. В этом пункте лабораторной работы мы рассмотрим как выполняется установка SSH в Ubuntu 20.04, а также поговорим о начальной настройке SSH сервера.

**Что такое SSH?**

SSH или Secure Shell - это протокол безопасного доступа из одного компьютера к другому по сети. У протокола SSH очень много возможностей. Вы можете создавать защищенные соединения между компьютерами, открывать командную строку на удаленном компьютере, запускать графические программы, передавать файлы и организовывать частные сети.

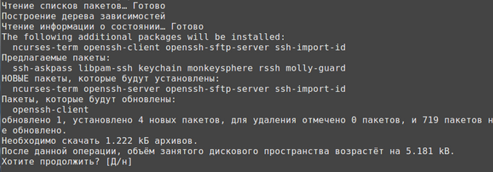
За поддержку протокола SSH в Linux отвечает набор программного обеспечения OpenSSH. Это открытая реализация этого протокола, которая предоставляет все необходимые возможности. В состав пакета OpenSSH входят утилиты для установки соединения, передачи файлов, а также сам ssh сервер.

**Установка OpenSSH в Ubuntu**

Установить SSH на Ubuntu будет очень просто, программа считается стандартной и используется почти везде. Хотя по умолчанию в дистрибутиве её нет, но зато она есть в официальных репозиториях.

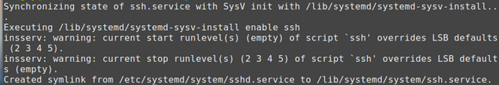
Поэтому для установки нужно открыть терминал с помощью сочетания клавиш Ctrl+Alt+T и выполнить команду:

*sudo apt install openssh-server*



Будет загружено несколько пакетов, а когда установка ssh сервера Ubuntu завершится, программа будет готова к работе. Чтобы служба запускалась автоматически, нужно добавить его в автозагрузку, поэтому чтобы включить SSH в Ubuntu 20.04 нужно выполнить:

*sudo systemctl enable sshd*



Если затем вы захотите удалить службу из автозагрузки, используйте команду disable:

*sudo systemctl disable sshd*

Что касается клиента ssh, то он уже установлен в системе по умолчанию. Сейчас можно попробовать подключиться к локальному ssh серверу просто набрав:

*ssh localhost*

Вы можете получить ssh доступ ubuntu к любому другому компьютеру из сети. Для этого достаточно указать вместо localhost его ip адрес и имя пользователя в таком формате:

*ssh имя\_пользователя@ip\_адрес*

3) Настройка удаленного доступа по протоколу SSH

С параметрами по умолчанию сервер SSH не очень безопасен поэтому перед тем, как программа будет готова к полноценному использованию ее нужно немного настроить. Все настройки сервера SSH хранятся в конфигурационном файле sshd\_config, который находится в папке /etc/ssh.

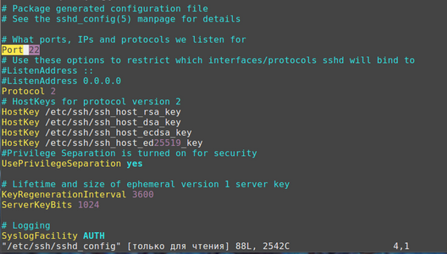
Перед тем как вносить изменения в этот конфигурационный файл рекомендуется сделать его резервную копию, для этого нужно использовать такую команду:

*sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.factory-defaults*

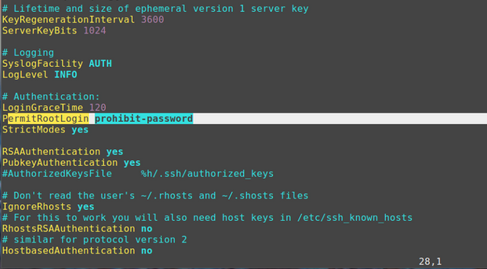
Дальше стоит перейти к настройке конфигурационного файла:

*sudo vi /etc/ssh/sshd\_config*

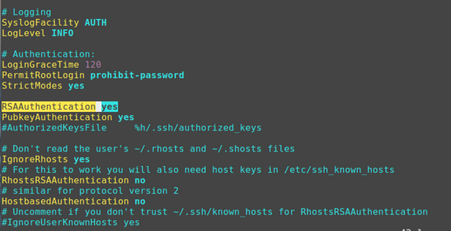
Первым делом желательно сменить порт, на котором работает ssh, возможный злоумышленник не знал включен ли у вас этот сервис. Найдите в конфигурационном файле строчку Port и замените ее значение на любое число, например, Port 2222:



По умолчанию вход от имени суперпользователя включен, рекомендуется отключить такую возможность. Для этого найдите строчку PermitRootLogin и замените ее значение на no:



Чтобы разрешить аутентификацию по ключу, а не по паролю найдите строку PubkeyAuthentication и убедитесь, что ее значение yes:



После того как все настройки будут завершены, сохраните изменения нажав: w и перезапустите службу SSH:

*sudo systemctl restart ssh*

Если вы изменили порт, то при подключении в клиенте тоже нужно указать новый порт, так как по умолчанию будет использоваться 22, например:

*ssh -p 2222 localhost*

Если на компьютере установлен и настроен брандмауэр, то в нем тоже нужно разрешить доступ к новому порту ssh, для этого выполните:

*sudo ufw allow 2222*

Даже если служба ssh находится на порту по умолчанию, его тоже нужно открыть в брандмауэре если вы собираетесь подключаться к компьютеру через интернет:

*sudo ufw allow 22*

Настройка ssh Ubuntu 20.04 полностью завершена.

Когда установка SSH в Ubuntu 20.04 завершена, вы можете получить удаленный доступ к своему компьютеру через интернет и быть уверенными что он находится в безопасности.