Лабораторная работа № 6.2

**Тема:** настройка сетевых протоколов для удалённого доступа в Linux.

**Цель:** изучить способы настройки компьютера с операционной системой Linux в качестве сервера и клиента протоколов telnet и SSH.

# Задание

Для выполнения данной работы необходимо, чтобы виртуальные машины имели как связь между собой, так и доступ в интернет. Для этого нужно использовать в VirtualBox тип сети либо «Мост», либо «Сеть NAT».

## 1 Настройка telnet

1.1 Установите службу telnet на Ubuntu Server:

sudo apt update

sudo apt install telnetd

Убедитесь, что сервер telnet запущен и ожидает подключений:

netstat –a | grep telnet

1.2 Выполните подключение по telnet из десктопной версии Linux к серверной версии. Для этого откройте терминал и введите команду:

telnet ip\_адрес\_сервера

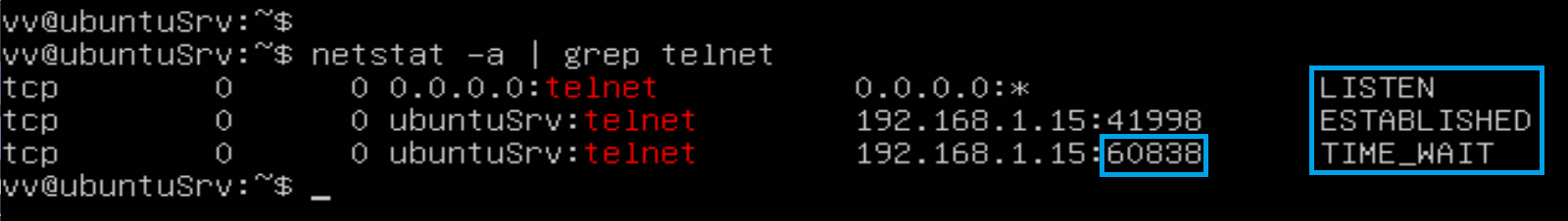
подставив в неё IP-адрес виртуальной машины с Ubuntu Server. Если соединение успешно, то должно появиться приглашение для ввода логин, а затем пароля.

1.3 Отключите telnet-соединение командой exit и установите его заново.

В серверной виртуальной машине снова выполните команду:

netstat –a | grep telnet

Примерные результаты выполнения данной команды показана на рисунке ниже. Объясните значения, обведённые синей рамкой.



## 2 Настройка SSH.

2.1 Установите службу, отвечающую за работу SSH на Ubuntu Server:

sudo apt install openssh-server

Убедитесь, что сервер SSH запущен:

sudo systemctl status ssh

В результатах работы команды должно быть написано зелёным «active(running)».

Убедитесь, что сервер готов принимать SSH-подключения:

netstat –a | grep ssh

2.2 Выполните подключение по SSH из десктопной версии Linux к серверной версии.

Если имя пользователя в обоих виртуальных машинах совпадают, то для подключения по SSH можно использовать команду:

ssh ip\_адрес\_сервера

Если пользователя, с таким же именем как на декстопной версии не существует на сервере, то в команде нужно явно указать имя пользователя сервера:

ssh пользователь@ip\_адрес\_сервера

Если сервер готов принять подключение, то появится запрос на добавление его ключа и необходимо будет ввести «yes».

*Аналогичным образом можно подключаться по SSH и из Windows. Для этого можно использовать либо специальные утилиты, например PuTTY, либо встроенный SSH-клиент, который появился начиная с версии Windows 10 1809.*

2.3 Настройте авторизацию по ключу вместо авторизации по паролю.

На десктопной версии Linux завершите SSH-подключение командой exit и выполните команду для генерации ключей:

ssh-keygen -t rsa

Затем отправьте ключ на сервер:

ssh-copy-id -i ~/.ssh/id\_rsa.pub пользователь@ip\_адрес\_сервера

В приведённой выше команде «~/.ssh/id\_rsa.pub» — стандартный путь к файлу с ключом. Если при генерации ключей в предыдущем пункте был задан другой путь, то следует указать его.

2.4 Ещё раз проверьте возможность подключения к серверу по SSH и убедитесь, что на этот раз пароль не потребуется и завершите SSH-соединение.

2.5 Отправьте файл по SSH с помощью утилиты «scp».

На десктопной версии Linux создайте простой текстовый файл с каким-либо текстом. Затем выполните команду:

scp file.txt пользователь@ip\_адрес\_сервера:~

Символ «~» после двоеточия указывает, что файл должен быть скопирован в домашнюю папку того пользователя, имя которого указано перед @. Вместо ~ можно указать и другой путь, убедившись, что у пользователя есть право на запись в указанный каталог.

На виртуальной машине убедитесь, что файл действительно скопировался.

2.6 Измените порт SSH.

Перейдите в папку /etc/ssh

Откройте файл sshd\_config

Найдите строку:

#Port 22

раскомментируйте её, убрав символ # в начале строки и замените число 22 на любой другой свободный порт.

Перезапустит службу sshd:

sudo systemctl restart sshd

2.7 Попытайтесь подключиться по SSH из десктопной версии Linux к серверной версии как это показано в пункте 2.2. При невозможности подключения добавьте к команде параметр -p число, где число соответствует тому, которое было вписано в файл с настройками.

2.8 Для того, чтобы доступ по SSH не пропал после перезагрузки, нужно включить «автозагрузку» службы sshd. Это делается командой:

sudo systemctl enable sshd

# Контрольные вопросы

1. В чём разница между telnet и SSH?

2. Что такое порт?

3. Какие порты используют по умолчанию telnet и SSH?

4. Какой командой в Linux можно проверить готова ли сетевая служба принимать соединения?

5. Какие способы аутентификации поддерживаются в SSH? В чём между ними разница?