Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

**Лабораторная работа №1**

По дисциплине: «Безопасность компьютерных систем и сетей»

Тема: «Настройка удаленного доступа к серверу с использованием SSH»

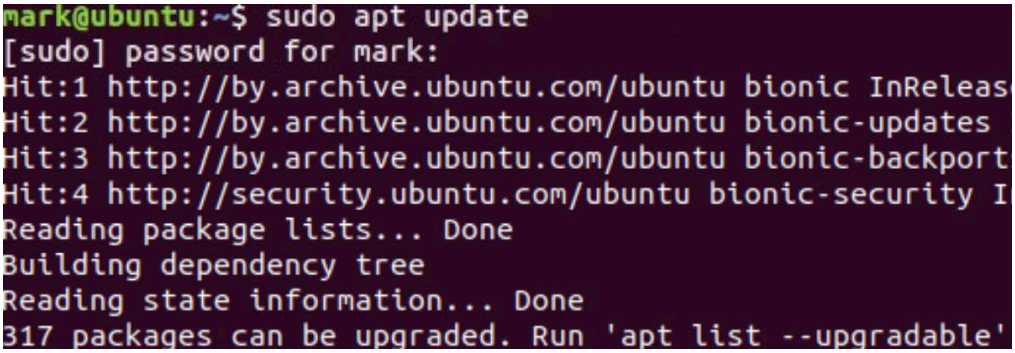
**Выполнил:**
Студент 4 курса
Группы ПО-7
Дмитрук М.А.
**Проверил:**
Самолюк О.Ю.

Брест, 2023

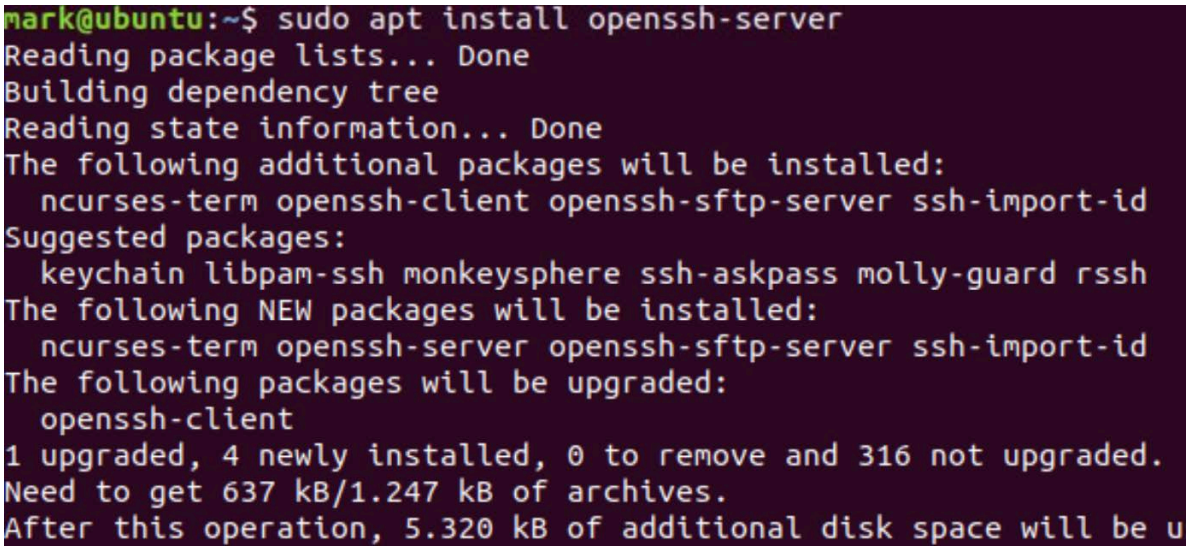
**Цель работы:** научиться подключаться по протоколу ssh к удаленному компьютеру. Уметь изменять конфигурацию Open SSH сервера под себя. Научиться выполнять дистанционно команды по ssh на удаленных компьютерах. Научиться устанавливать удаленное соединение по ключу без ввода логина и пароля. Ознакомиться с пользовательскими файлами конфигурации ssh. Использовать SFTP.

**Ознакомление с ssh сервером.**

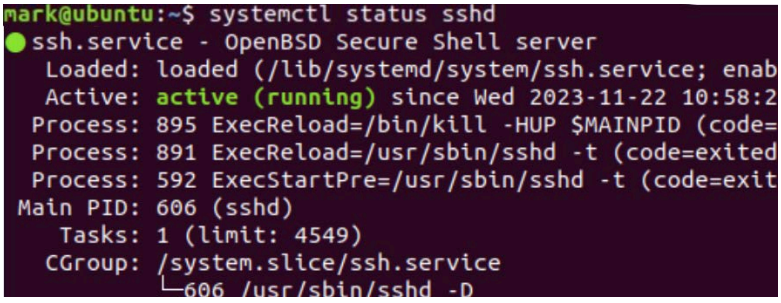
1. Перейдите в командную строку виртуальной машины. Обновите информацию о пакетах выполнив команду apt update.




2. Установите Open SSH если он не установлен.

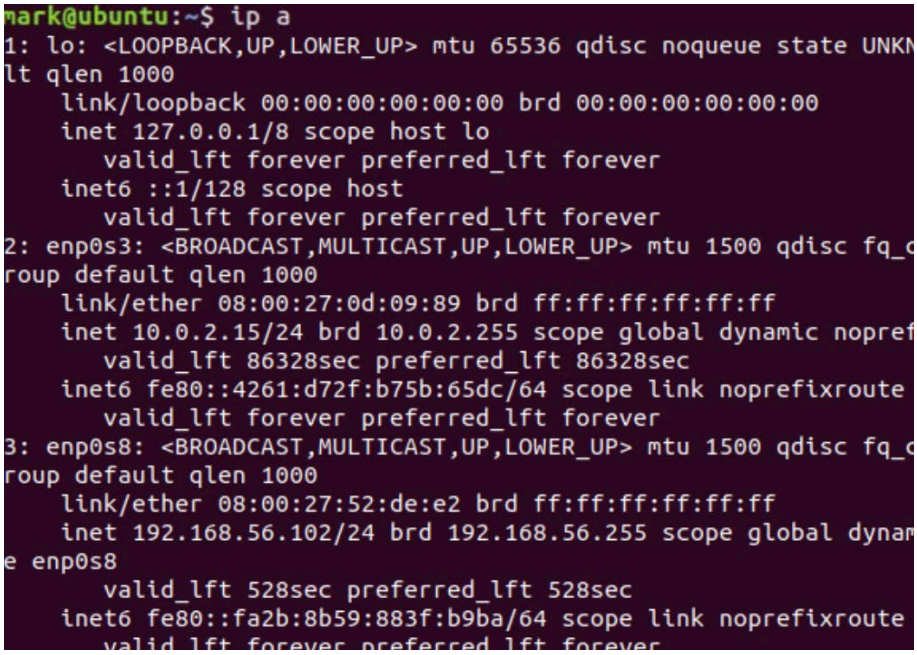



3. Используйте команду systemctl status sshd чтобы посмотреть состояние службы ssh.

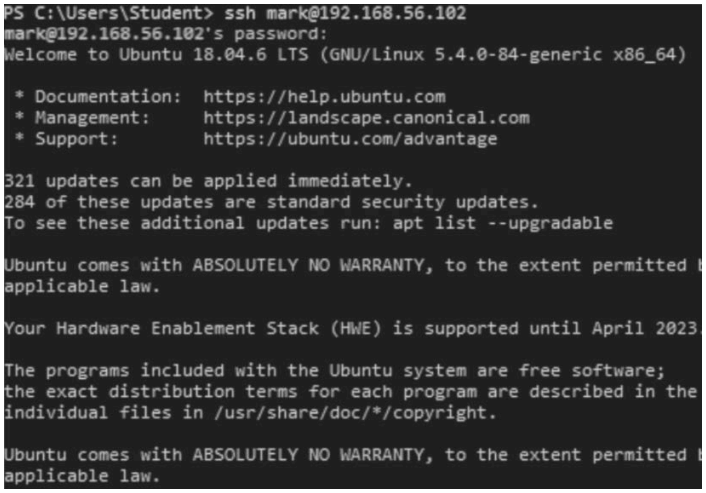


4. **Если пароль для root не задан.** Перейдите в root пользователя sudo su и используйте команду passwd чтобы задать пароль.

5. Смотрим IP адрес командой ip a.




6. С основного компьютера подключаемся по ssh используя команду **ssh root@ip_удаленной_машины**. Нажимаем Y. Вводим пароль.




7. Почитайте файл конфигурации. Измените порт по умолчанию. Смена порта связана с тем, что многочисленные сетевые сканеры постоянно пытаются соединиться с 22-м портом и как минимум получить доступ путем перебора логинов/паролей из своей базы. Даже если у вас и отключена парольная аутентификация — эти попытки сильно засоряют журналы и (в большом количестве) могут негативно повлиять на скорость работы ssh сервера. Для лучшей защиты настраивают fail2ban для защиты ssh от перебора паролей. Сделайте так что бы было нельзя подключиться по root пользователю.

```
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

8. Перезагрузите **sshd**. Для этого воспользуйтесь **systemctl**. Также проверьте состояние службы.

```
mark@ubuntu:~$ systemctl restart sshd
mark@ubuntu:~$ systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; e
   Active: active (running) since Wed 2023-11-22 11:1
  Process: 895 ExecReload=/bin/kill -HUP $MAINPID (co
  Process: 891 ExecReload=/usr/sbin/sshd -t (code=exi
  Process: 2075 ExecStartPre=/usr/sbin/sshd -t (code=
 Main PID: 2076 (sshd)
    Tasks: 1 (limit: 4549)
   CGroup: /system.slice/ssh.service
           └─2076 /usr/sbin/sshd -D
```

9. Отобразите в отчете результат изменений. Чтобы узнать как подключиться с другим портом почитайте man по команде ssh или воспользуйтесь поисковиком.

```
PS C:\Users\Student> ssh mark@192.168.56.102
ssh: connect to host 192.168.56.102 port 22: Connection refused
PS C:\Users\Student> ssh mark@192.168.56.102 -p 2222
mark@192.168.56.102's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

321 updates can be applied immediately.
284 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Wed Nov 22 11:02:07 2023 from 192.168.56.1
```

10. Верните порт по умолчанию на стандартный порт **ssh**. Перезагрузите службу.

**Подключение по ключу.**

1. Выполните команду **ssh-keygen** для создания ключа на основной машине. Утилита спросит вас, куда сохранить создаваемый закрытый ключ. По умолчанию (если нажмете ENTER), ключ будет сохранен в папку **.ssh** вашего домашнего каталога. Следующим шагом вам будет предложено установить пароль на закрытый ключ. Пароль будет запрашиваться при каждом использовании этого закрытого ключа. Установка пароля необязательна (можно просто нажать ENTER), но необходимо учесть, что любой человек, к которому попадет не защищенный паролем закрытый ключ, сможет получить доступ к вашему серверу. Установив (или не установив) пароль, вы завершите процедуру генерации SSH-ключей. Если в процессе не указывали иного, создадутся следующие файлы:

- Закрытый ключ: ~/.ssh/id_rsa
- Открытый ключ: ~/.ssh/id_rsa.pub

```
PS C:\Users\Admin> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Admin/.ssh/id_rsa):
C:\Users\Admin/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Admin/.ssh/id_rsa.
Your public key has been saved in C:\Users\Admin/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:KRceUJBU1vf62G5VJjWDj1DP67WW11Rv3YhYTU4hwUM admin@WIN-9HQG3I9QID3
The key's randomart image is:
+---[RSA 2048]----+
|     .+=+..+E.=. |
|      .o .. *B o.|
|        o ..+=o.+|
|       . + + o+.B|
|      . S . .o.+B|
|       o    o .o=|
|             = =o|
|            . = .|
|             o.  |
+----[SHA256]-----+
```

2. Теперь вам необходимо скопировать открытый ключ на сервер. Для этого выполните следующую команду: **ssh-copy-id username@ipserver**. Вам понадобится ввести пароль этого пользователя. После этого содержимое локального файла ~/.ssh/id_rsa.pub будет добавлено в файл ~/.ssh/authorized_keys домашнего каталога соответствующего пользователя на сервере.

```
PS C:\Users\Student> cat C:\Users\Student\.ssh\id_rsa.pub | ssh mark@192.168.56.102 "mkdir ~/.ssh; cat >> ~/.ssh/authorized_keys"
mark@192.168.56.102's password:
```

3. Теперь вы можете авторизоваться на сервере с помощью SSH-ключей с помощью команды: ssh username@ipserver. Без ввода пароля.

```
PS C:\Users\Student> ssh mark@192.168.56.102
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

321 updates can be applied immediately.
284 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Wed Nov 22 11:37:54 2023 from 192.168.56.1
```

4. После того как проверили авторизацию по ssh ключу отключите авторизацию по логину и паролю. Для этого вам понадобится отредактировать файл **/etc/ssh/sshd_config** на вашей виртуальной машине. В файле необходимо найти директиву **PasswordAuthentication**, раскомментировать ее, если она закомментирована, и установить для нее значение «**no**»

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

**Удаленный запуск команд.**

1. Для удаленного запуска команд используют следующий синтаксис **ssh USER@HOST ‘command’**. Выполните удаленную установку какого-либо пакета к примеру mc. Подобный способ выполнения удалённых команд может быть использоваться для создание скриптов.

2. cat C:\Users\Student\.ssh\id_rsa | ssh mark@192.168.56.102 "echo '1234' | sudo -S apt install -y mc"

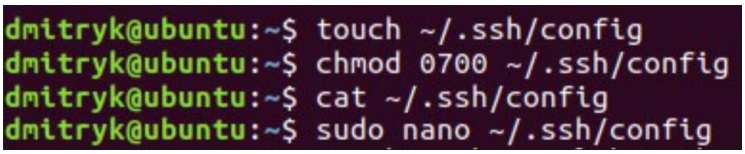
```
PS C:\Users\Student> cat C:\Users\Student\.ssh\id_rsa | ssh mark@192.168.56.102 "echo '1234' | sudo -S apt install -y
mc"
[sudo] password for mark:
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists...
Building dependency tree...
Reading state information...
The following additional packages will be installed:
  libssh2-1 mc-data
Suggested packages:
  arj catdvi | texlive-binaries dbview djvulibre-bin gv libaspell-dev links
  | w3m | lynx odt2txt python python-boto python-tz
The following NEW packages will be installed:
  libssh2-1 mc mc-data
0 upgraded, 3 newly installed, 0 to remove and 316 not upgraded.
Need to get 1.712 kB/1.785 kB of archives.
After this operation, 7.542 kB of additional disk space will be used.
Get:1 http://by.archive.ubuntu.com/ubuntu bionic/universe amd64 mc-data all 3:4.8.19-1 [1.238 kB]
```

**Пользовательские файлы конфигурации ssh.**

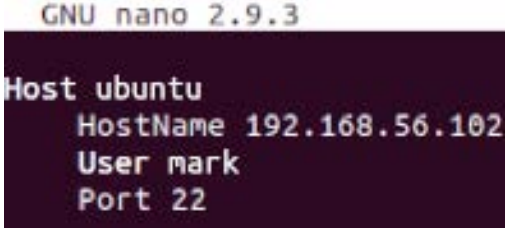
1. Необходима 2-я машина с Linux. Сгенерируйте ssh ключ и передайте на 2 машину. Чтобы реализовать подключение по ключу.

Тестирование будет производиться с одной машиной, т.к в установке второй машины ради второго копирования ключа нет смысла

2. Пользовательский файл обычно не создается по умолчанию, поэтому вам нужно создать его с разрешениями на чтение и запись только для пользователя. Воспользуйтесь следующими командами:




Вышеупомянутый файл содержит разделы, определенные спецификациями хостов, и раздел применяется только к хостам, которые соответствуют одному из шаблонов, заданных в спецификации.




**Настройте файл конфигурации для подключения к виртуальной машине 2. Хостнейм ваша фамилия**

Теперь вы сможете подключаться к серверу просто вписав hostname к примеру так **ssh ubuntu**. В отчете отобразите что у вас удалось подключиться по hostname. Такой способ удобен когда вам необходимо администрировать большое количество серверов. Вам не приходиться запоминать логины пароли порт для конкретного сервера а также IP адрес.

```
dmitryk@ubuntu:~$ ssh ubuntu
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

321 updates can be applied immediately.
284 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted b
applicable law.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Wed Nov 22 12:49:34 2023 from 192.168.56.101
```

**Работа с SFTP**

1. Выполните подключение по sftp. sftp username@ipserver.

```
dmitryk@ubuntu:~$ sftp ubuntu
Connected to ubuntu
sftp>
```

2. Оказавшись в командной строке sftp можно получить список доступных команд с помощью команды help.

```
sftp> help
Available commands:
bye                                Quit sftp
cd path                            Change remote directory to 'path'
chgrp grp path                     Change group of file 'path' to 'grp'
chmod mode path                    Change permissions of file 'path' to 'mode'
chown own path                     Change owner of file 'path' to 'own'
df [-hi] [path]                    Display statistics for current directory or
                                   filesystem containing 'path'
exit                               Quit sftp
get [-afPpRr] remote [local]       Download file
reget [-fPpRr] remote [local]      Resume download file
reput [-fPpRr] [local] remote      Resume upload file
help                               Display this help text
lcd path                           Change local directory to 'path'
lls [ls-options [path]]            Display local directory listing
lmkdir path                        Create local directory
ln [-s] oldpath newpath            Link remote file (-s for symlink)
lpwd                               Print local working directory
ls [-1afhlnrSt] [path]             Display remote directory listing
lumask umask                       Set local umask to 'umask'
mkdir path                         Create remote directory
progress                           Toggle display of progress meter
put [-afPpRr] local [remote]       Upload file
pwd                                Display remote working directory
```

3. Посмотрите текущей рабочий каталог на своем и удаленном пк.

```
sftp> pwd
Remote working directory: /home/mark
sftp> lpwd
Local working directory: /home/dmitryk
```

4. Попробуйте изменить рабочую директорию на своем и удаленном пк.

```
sftp> pwd
Remote working directory: /
sftp> lpwd
Local working directory: /home/dmitryk/Documents
```

5. Для того чтобы передать файл по sftp используйте команду put. Для передачи папки используйте ключ -r.

Передадим файл:

```
sftp> put test.txt
Uploading test.txt to /home/mark/test.txt
test.txt                                      100%    0     0.0KB/s   00:00
```

```
sftp> put -r directory
Uploading directory/ to /home/mark/directory
Entering directory/
```

6. Для того чтобы скачать что то с удаленного сервера используйте команду get. Для загрузки директории используйте ключ -r.

```
sftp> get test.txt
Fetching /home/mark/test.txt to test.txt
```

```
sftp> get -r directory
Fetching /home/mark/directory/ to directory
Retrieving /home/mark/directory
```

7. Создайте и удалите директорию на удаленным пк (ВМ) в sftp.

```
sftp> mkdir test-remove
sftp> ls
Desktop             Documents           Downloads           Music
Pictures            Public              Templates           Videos
directory           examples.desktop    test                test-remove
test.txt
sftp> rmdir test-remove
sftp> ls
Desktop             Documents           Downloads           Music
Pictures            Public              Templates           Videos
directory           examples.desktop    test                test.txt
```

**Вывод:** научился подключаться по протоколу ssh к удаленному компьютеру и изменять конфигурацию Open SSH сервера под себя. Научился выполнять дистанционно команды по ssh на удаленных компьютерах и устанавливать удаленное соединение по ключу без ввода логина и пароля. Ознакомился с пользовательскими файлами конфигурации ssh и использованием SFTP.