PW-02. USING SSH/RDP FOR REMOTE LINUX/UNIX/MAC/WINDOWS SERVERS MANAGEMENT.

1. PURPOSE OF WORK

Get the initial skills of working with a remote host via ssh protocol. Secure SHell is the primary means of remotely managing networked computers running UNIX/Linux.

The Linux/UNIX commands are used: **ssh, scp, uname, passwd, date, who, pwd, mkdir, mc, exit, logout**.

2. TASKS FOR WORK

2.1. Install **Secure Shell Extension** on your Chrome browser in the classroom or at home.

Using the Secure Shell Extension, connect to the remote server with your training account (login and password).

Use the **uname** command (with the appropriate parameters: -o, -I, -m, -p, -r, -v, -s, -n) to determine the type of operating system, hardware platform, release, version & name of the kernel, node name for remote Linux (make a Screenshot 1).

2.2. Download **Putty.exe** on your Windows computer in the classroom or at home.

Using the **putty.exe**, connect to the remote server with your training account (login and password).

Use the **passwd** command for change your password on remote server.

Use the **date** command (with the appropriate parameters) to determine the date and time of the remote server (make a Screenshot 2).

2.3. Start Your **Linux Virtual Machine** on VirtualBox on your Windows computer (show Lab Work 01). Start Linux Terminal.

2.4. Use the **uname** command (with the appropriate parameters: -o, -I, -m, -p, -r, -v, -s, -n) to determine the type of operating system, hardware platform, release, version & name of the kernel, node name for local Linux (make a Screenshot 3).

2.5. Use the **ssh** command on Linux Virtual Machine (without loading the remote server shell) to determine the date and time (date command with the appropriate parameters) for remote server (make a Screenshot 4).

2.6. Using the **ssh** client on Linux Virtual Machine, connect to the remote server with your training account. Determine which users, in which terminals and from which ip-addresses are connected to the server (**who** command) (make a Screenshot 5).

2.7. Using the **ssh** client on Linux Virtual Machine, connect to the remote server with your training account.

Determine which directory is current on the remote server (**pwd**). If it is different from /home/stYYNN, then go to /home/stYYNN. In the Your home directory, create subdirectory (**mkdir**) as your transliteration_surname (for example, ivanov).

Run the **mc** file manager on remote server, view the contents of the current directory (make a Screenshot 6).

Finish working with the mc file manager (F10 or **exit**). End the ssh session (**logout**).

2.8. Using the **mc** command on Linux Virtual Machine configure **SFTP connection** to remote server. Copy any file from local Linux to remote server and back from remote to local (make a Screenshot 7).

2.9. Use the **ssh** command on Linux Virtual Machine (without loading the remote server shell), upload an arbitrary file (**scp** command) to the directory you previously created on the remote server. Without entering an ssh session on the remote server, view the contents of the server directory /home/stYYNN (make a Screenshot 8).

2.10. Yourself need learn how to transfer files from/to a remote server using the **Secure Shell Extension** for Chrome and **WinSCP.exe** for Windows.

3. Report

Make a report about this work (Screenshots 1-8) and send it to the teacher’s email.

Report for Lab Work 03: Using SSH/RDP for remote Linux/UNIX /Mac/Windows servers management

Student Name Surname	Student ID	Date

Screenshot 1	Screenshot 2
…	…
Screenshot 7	Screenshot 8

4. GUIDELINES

Remote server management tools are widely used in both local and global networks. One of the main requirements for remote control programs is user transparency and low traffic. This allows you to centrally manage geographically distributed nodes from one workstation or provide access to remote terminal clients via slow communication lines.

For management, both symbolic protocols (telnet, rlogin, ssh) and binary protocols that support graphical capabilities (many different ones) are used. For dedicated servers, graphical tools are generally not used, since such servers do not imply their use as workstations. This means that there is no need to devote significant resources to the graphical user interface.

The telnet and rlogin text protocols are simple and functional, but unsafe, so remote management of a UNIX server using the ssh protocol is assumed. It should be noted that the ssh protocol also supports working with graphical mode (tunneling of the X server). Moreover, the ssh protocol allows you to tunnel any network traffic that uses the TCP protocol as a transport. (For details, see The Secure Shell (SSH) Protocol Assigned Numbers, RFC 4250, 2006; The Secure Shell (SSH) Protocol Architecture, RFC 4251, 2006; The Secure Shell (SSH) Authentication Protocol, RFC 4252, 2006, etc.).

To manage the server via ssh protocol, its support by the server and client ssh-application are necessary. UNIX servers support ssh as standard. As a client, OpenSSH is usually used (called by the ssh command). For Windows, there are clients from different manufacturers, the most popular PuTTY and SecureCRT. There is also an extension for the Chrome browser (Secure Shell Extension).

In the laboratory, it is planned to use the OpenSSH client and the Secure Shell Extension for Linux/UNIX/Mac, PuTTY for Windows and the Secure Shell Extension for Chrome.

Read before Lab

- How To Use SSH To Connect To A Remote Server In Linux Or Windows
  https://phoenixnap.com/kb/ssh-to-connect-to-remote-server-linux-or-windows
- 5 Linux SSH Security Best Practices To Secure Your Systems
  https://phoenixnap.com/kb/linux-ssh-security
- How To Generate SSH Keys On Ubuntu 18.04
  https://phoenixnap.com/kb/generate-setup-ssh-key-ubuntu
- 19 Common SSH Commands In Linux With Examples
  https://phoenixnap.com/kb/linux-ssh-commands

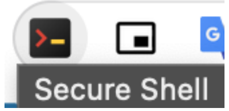
4.1. Linux Remote Server Connection.

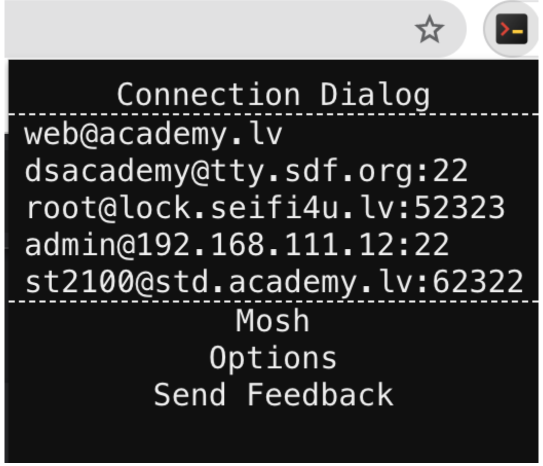
4.1.1. Secure Shell Extension for Chrome

1. Install the Secure Shell Extension for your browser Chrome.

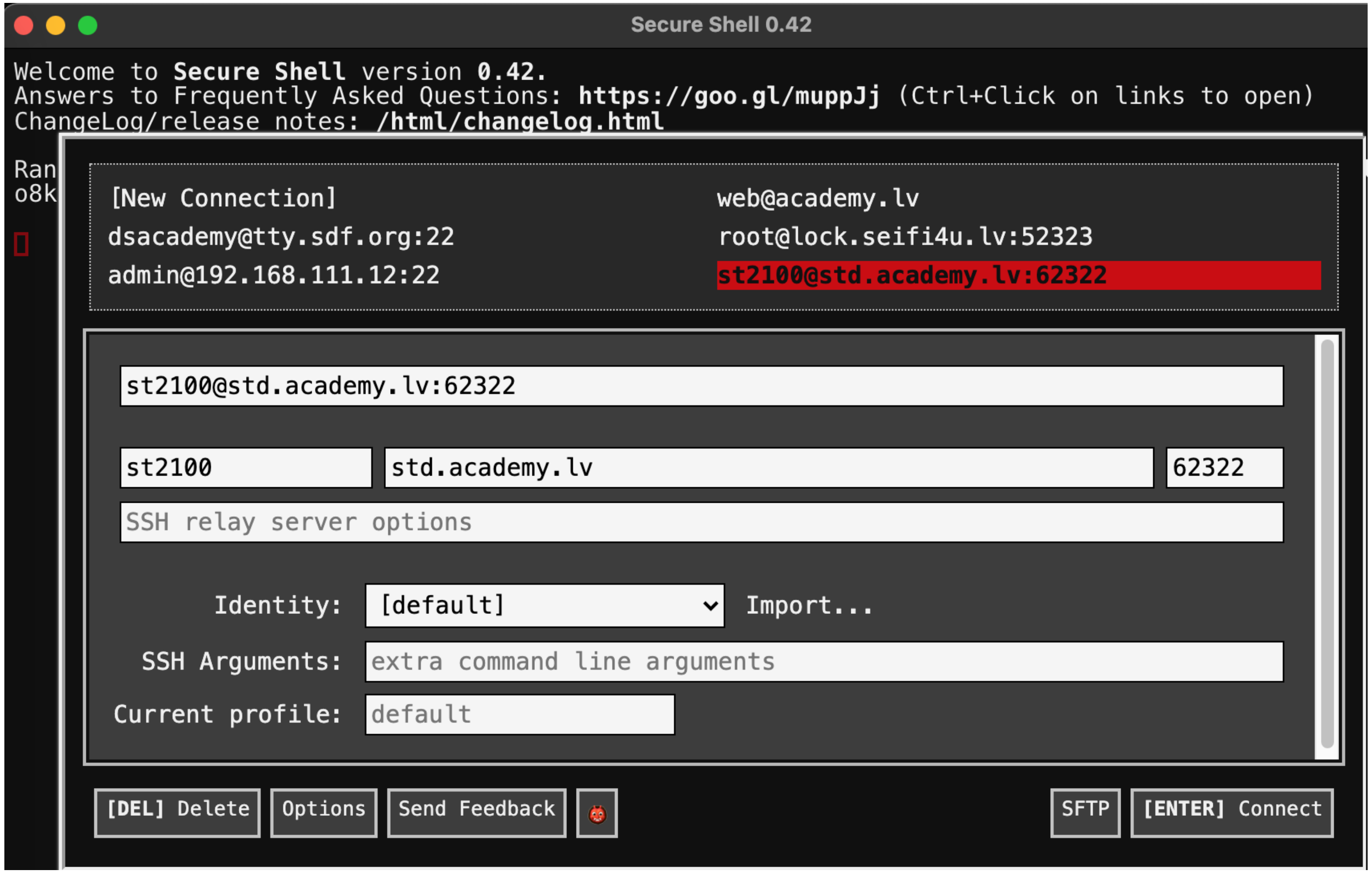
Link: https://chrome.google.com/webstore/detail/secure-shell-extension/iodihamcpbpeioajjeobimgagajmlibd

2. Run Secure Shell Extension and create a connection to remote server with parameters stYYNN@std.academy.lv:62322 , where YYNN – student year and number





```
Connection Dialog
web@academy.lv
dsacademy@tty.sdf.org:22
root@lock.seifi4u.lv:52323
admin@192.168.111.12:22
st2100@std.academy.lv:62322
Mosh
Options
Send Feedback
```



```
Welcome to Secure Shell version 0.42.
Answers to Frequently Asked Questions: https://goo.gl/muppJj (Ctrl+Click on links to open)
ChangeLog/release notes: /html/changelog.html

Ran
o8k
```

```
[New Connection]                    web@academy.lv
dsacademy@tty.sdf.org:22            root@lock.seifi4u.lv:52323
admin@192.168.111.12:22             st2100@std.academy.lv:62322
```

st2100@std.academy.lv:62322

st2100 | std.academy.lv | 62322

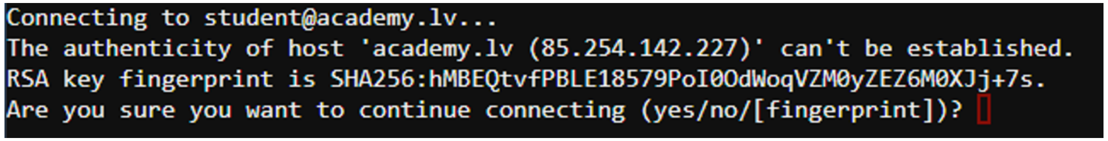
SSH relay server options

Identity: [default] Import...

SSH Arguments: extra command line arguments

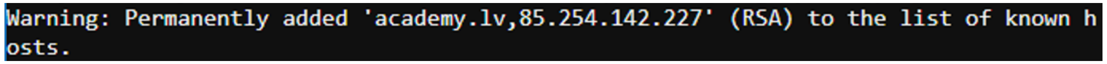
Current profile: default

3. When you first ssh connect to a remote machine, you will see a similar message:



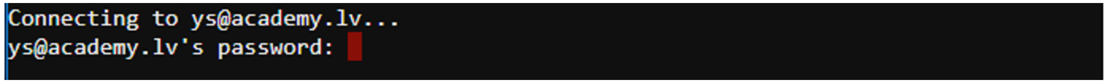
```
Connecting to student@academy.lv...
The authenticity of host 'academy.lv (85.254.142.227)' can't be established.
RSA key fingerprint is SHA256:hMBEQtvfPBLE18579PoI0OdWoqVZM0yZEZ6M0XJj+7s.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Enter yes to continue. In this case, the remote server will be added to your list of known servers, as indicated by the following message:



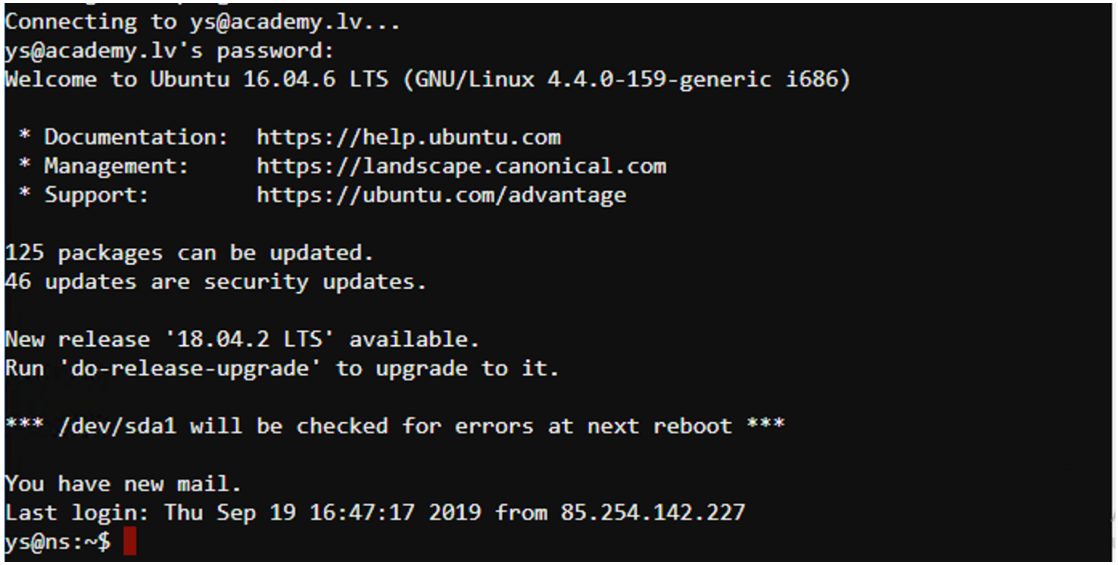
```
Warning: Permanently added 'academy.lv,85.254.142.227' (RSA) to the list of known h
osts.
```

4. Then you need to enter the password for the remote computer. Note that when entering the password, it does not print on the screen!



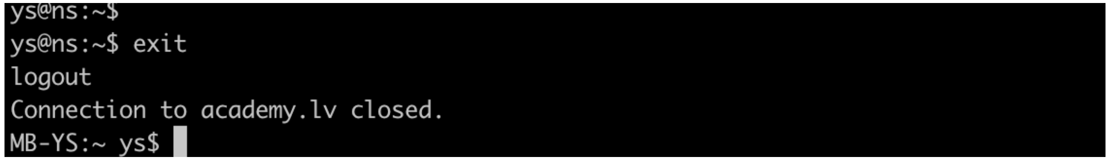
```
Connecting to ys@academy.lv...
ys@academy.lv's password:
```

5. After authorization on the remote server, the user enters the Linux/UNIX shell (bash) and can proceed to enter commands.



```
Connecting to ys@academy.lv...
ys@academy.lv's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic i686)

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

125 packages can be updated.
46 updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** /dev/sda1 will be checked for errors at next reboot ***

You have new mail.
Last login: Thu Sep 19 16:47:17 2019 from 85.254.142.227
ys@ns:~$
```

6. Logout from ssh. To complete the work using the ssh protocol, you must execute the exit or logout command, which ends the user session and terminates the connection:



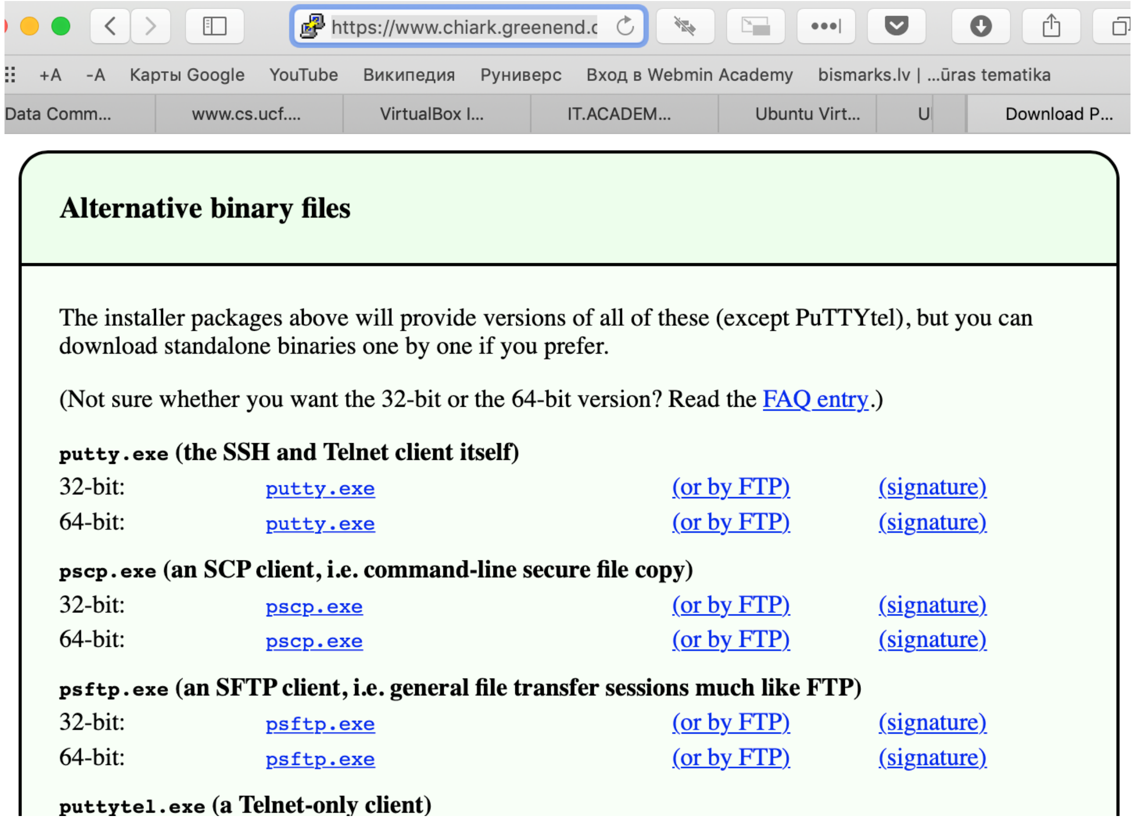
```
ys@ns:~$
ys@ns:~$ exit
logout
Connection to academy.lv closed.
MB-YS:~ ys$
```

4.1.2. PuTTY for Windows

1. Download Putty.exe for Windows OS (without installing to computer).

Link: see section “Download Alternative Binary Files for PuTTY (Windows)” on https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

2. Run Putty.exe for Windows OS and Create a connection to remote server with parameters stYYNN@std.academy.lv:62322.



Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel), but you can download standalone binaries one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

`putty.exe` (the SSH and Telnet client itself)

32-bit:	`putty.exe`	(or by FTP)	(signature)
64-bit:	`putty.exe`	(or by FTP)	(signature)

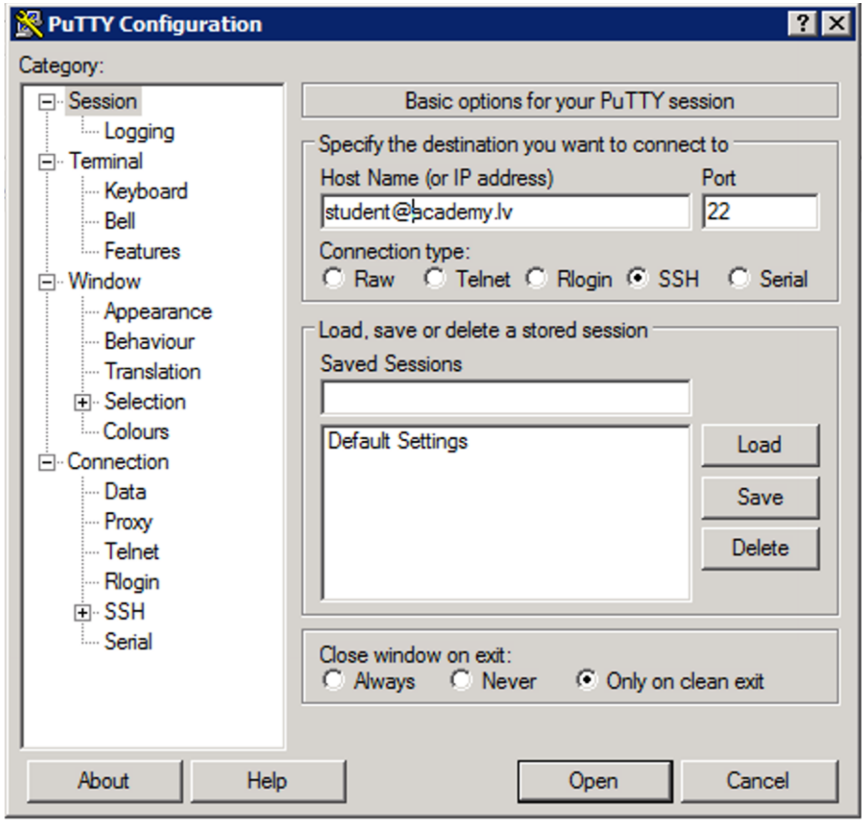
`pscp.exe` (an SCP client, i.e. command-line secure file copy)

32-bit:	`pscp.exe`	(or by FTP)	(signature)
64-bit:	`pscp.exe`	(or by FTP)	(signature)

`psftp.exe` (an SFTP client, i.e. general file transfer sessions much like FTP)

32-bit:	`psftp.exe`	(or by FTP)	(signature)
64-bit:	`psftp.exe`	(or by FTP)	(signature)

`puttytel.exe` (a Telnet-only client)



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): student@academy.lv

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

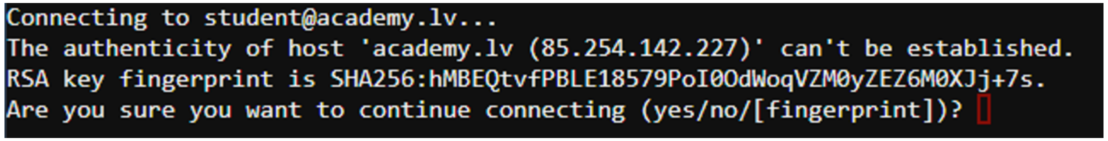
Load, save or delete a stored session

Saved Sessions:

Default Settings

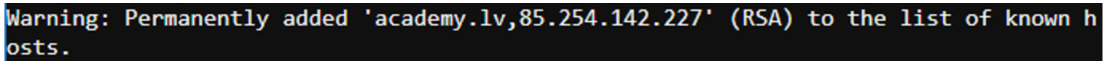
Close window on exit: ○ Always ○ Never ● Only on clean exit

3. When you first ssh connect to a remote machine, you will see a similar message:



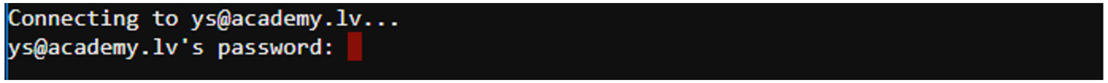
```
Connecting to student@academy.lv...
The authenticity of host 'academy.lv (85.254.142.227)' can't be established.
RSA key fingerprint is SHA256:hMBEQtvfPBLE18579PoI0OdWoqVZM0yZEZ6M0XJj+7s.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Enter yes to continue. In this case, the remote server will be added to your list of known servers, as indicated by the following message:



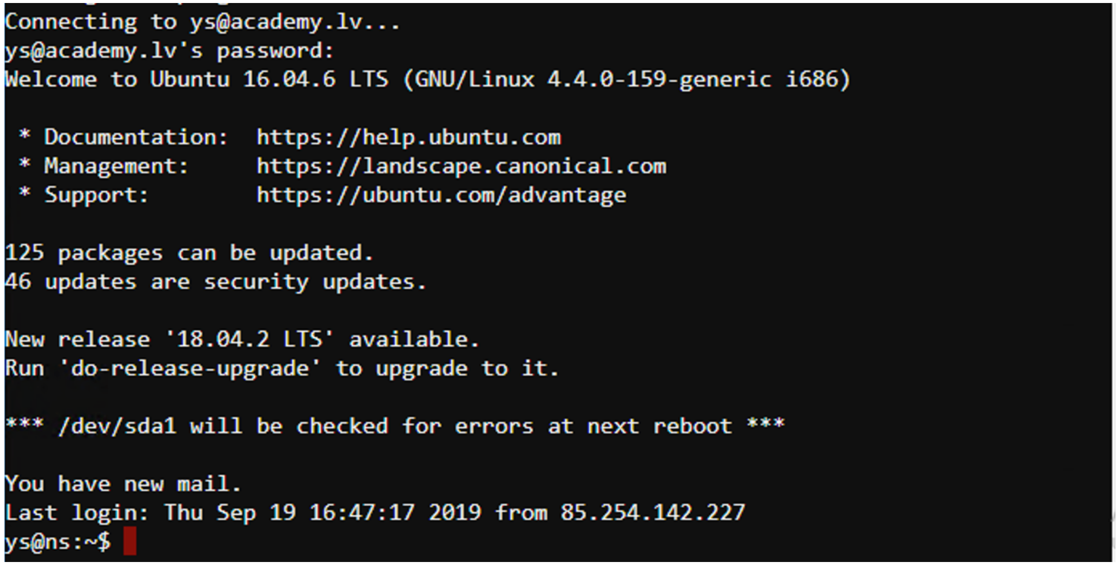
```
Warning: Permanently added 'academy.lv,85.254.142.227' (RSA) to the list of known h
osts.
```

4. Then you need to enter the password for the remote computer. Note that when entering the password, it does not print on the screen!



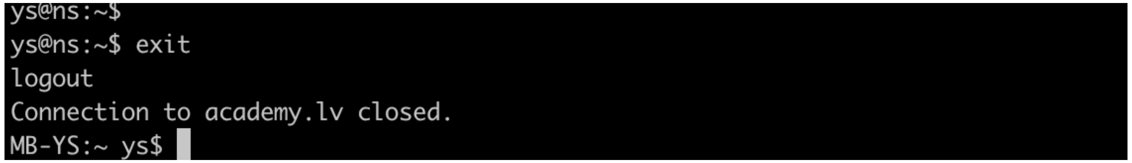
```
Connecting to ys@academy.lv...
ys@academy.lv's password:
```

5. After authorization on the remote server, the user enters the Linux/UNIX shell (bash) and can proceed to enter commands.



```
Connecting to ys@academy.lv...
ys@academy.lv's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic i686)

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

125 packages can be updated.
46 updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** /dev/sda1 will be checked for errors at next reboot ***

You have new mail.
Last login: Thu Sep 19 16:47:17 2019 from 85.254.142.227
ys@ns:~$
```

6. Logout from ssh. To complete the work using the ssh protocol, you must execute the exit or logout command, which ends the user session and terminates the connection:



```
ys@ns:~$
ys@ns:~$ exit
logout
Connection to academy.lv closed.
MB-YS:~ ys$
```

4.1.3. OpenSSH on Linux/UNIX/Mac

1. Install and run your Linux Virtual Machine.

Link: see Lab Work “Install Virtual Machines on Oracle VirtualBox”.

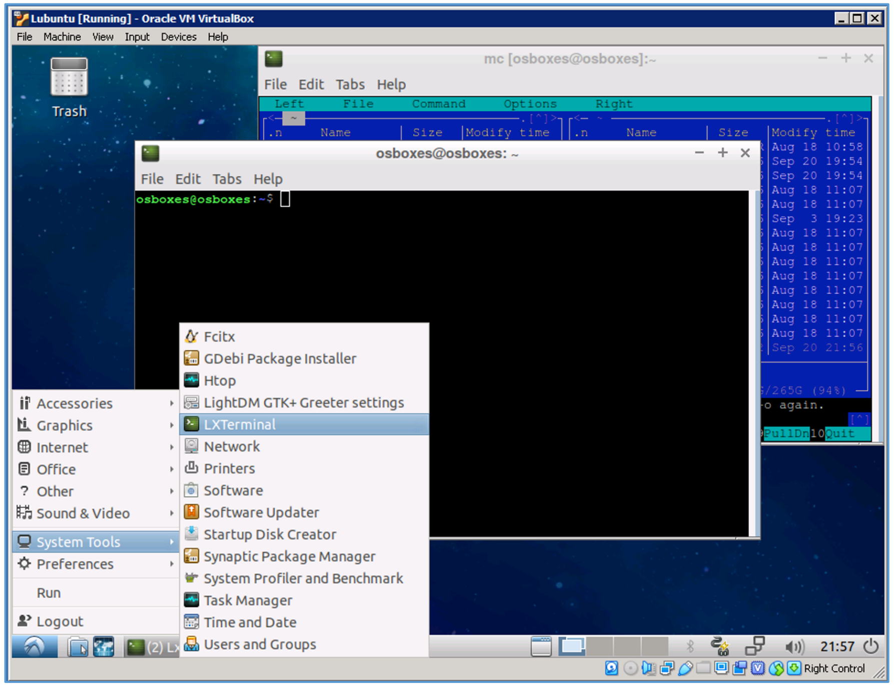
2. Launch a text terminal on your Linux Virtual and execute the ssh command with parameters stYYNN@std.academy.lv:62322

stud@comp:~> ssh -l stYYNN std.academy.lv -p 62322 // -l stYYNN – login name; std.academy.lv - ssh server name; -p 62322 – port number

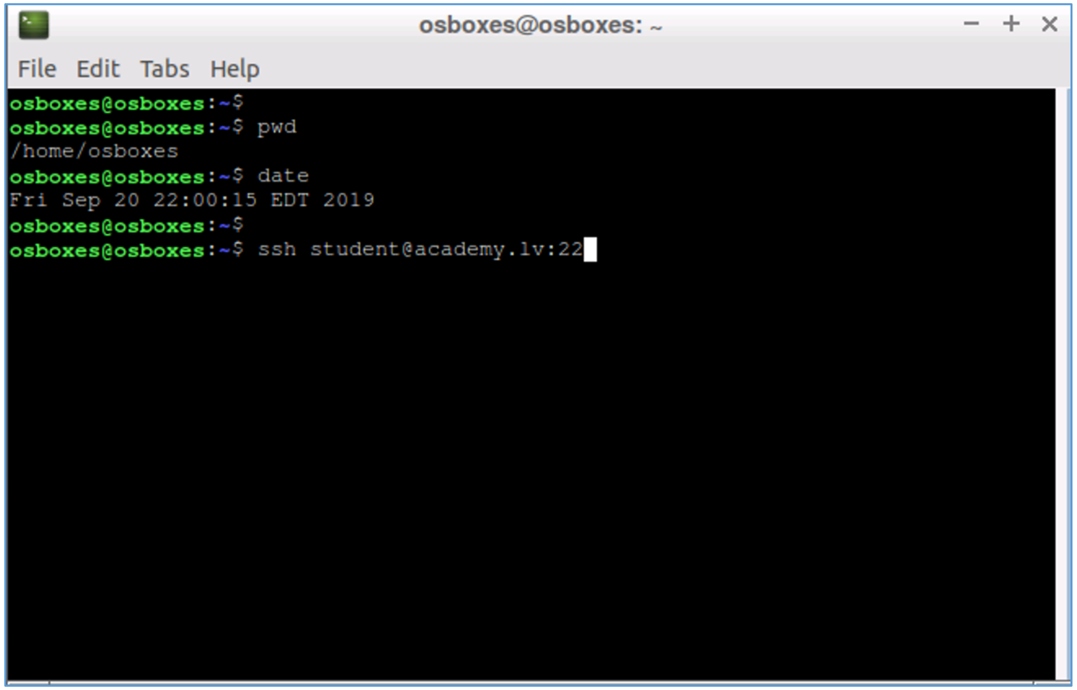
or so:

stud@comp:~> ssh stYYNN@std.academy.lv:62322

If you execute ssh without specifying a username, the server will be sent the name of the current local user (stud).

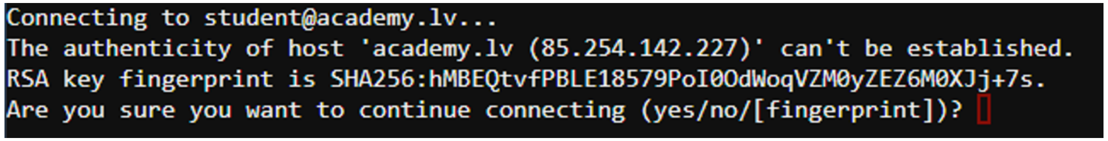


```
osboxes@osboxes:~$
```



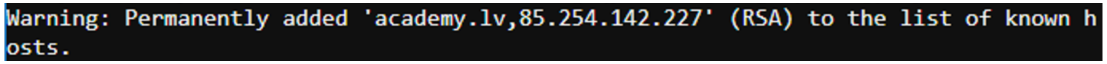
```
osboxes@osboxes:~$
osboxes@osboxes:~$ pwd
/home/osboxes
osboxes@osboxes:~$ date
Fri Sep 20 22:00:15 EDT 2019
osboxes@osboxes:~$
osboxes@osboxes:~$ ssh student@academy.lv:22
```

3. When you first ssh connect to a remote machine, you will see a similar message:



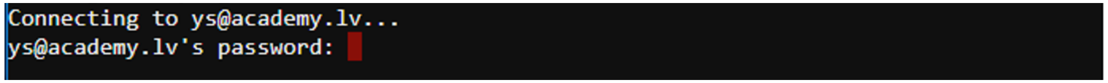
```
Connecting to student@academy.lv...
The authenticity of host 'academy.lv (85.254.142.227)' can't be established.
RSA key fingerprint is SHA256:hMBEQtvfPBLE18579PoI0OdWoqVZM0yZEZ6M0XJj+7s.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Enter yes to continue. In this case, the remote server will be added to your list of known servers, as indicated by the following message:



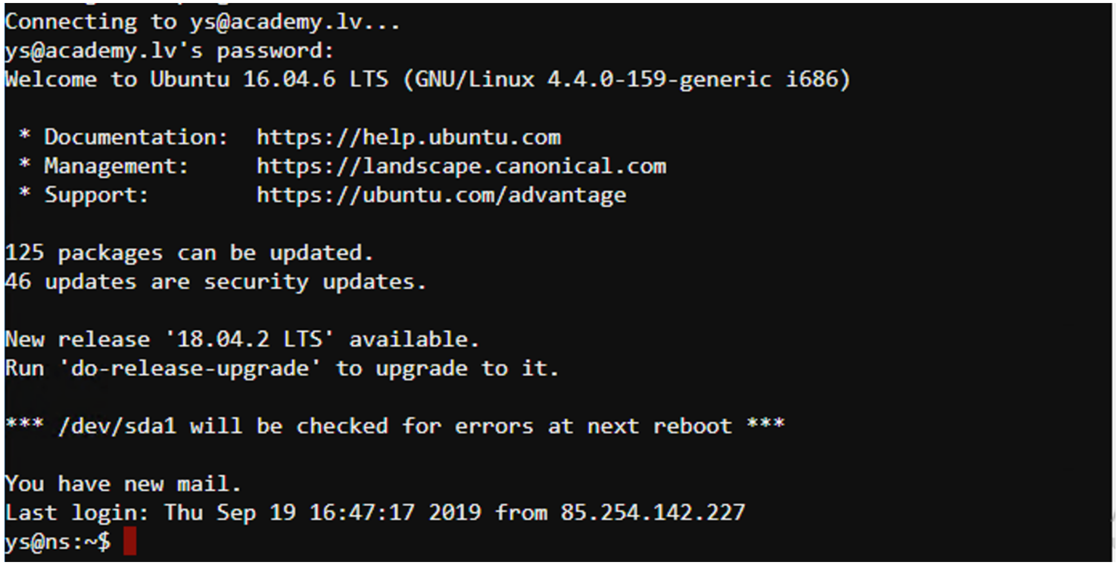
```
Warning: Permanently added 'academy.lv,85.254.142.227' (RSA) to the list of known h
osts.
```

4. Then you need to enter the password for the remote computer. Note that when entering the password, it does not print on the screen!



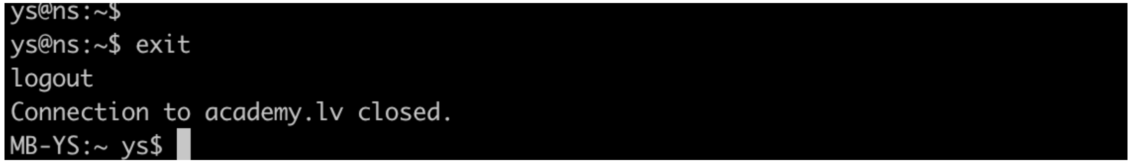
```
Connecting to ys@academy.lv...
ys@academy.lv's password:
```

5. After authorization on the remote server, the user enters the Linux/UNIX shell (bash) and can proceed to enter commands.



```
Connecting to ys@academy.lv...
ys@academy.lv's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic i686)

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

125 packages can be updated.
46 updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** /dev/sda1 will be checked for errors at next reboot ***

You have new mail.
Last login: Thu Sep 19 16:47:17 2019 from 85.254.142.227
ys@ns:~$
```

6. Logout from ssh. To complete the work using the ssh protocol, you must execute the exit or logout command, which ends the user session and terminates the connection:



```
ys@ns:~$
ys@ns:~$ exit
logout
Connection to academy.lv closed.
MB-YS:~ ys$
```

4.2. LINUX TERMINAL COMMAND EXECUTION.

For the user, the execution of commands on a remote server is not much different from the usual work with local commands and files. Here are a few examples:

4.2.1. DEFINITION OF THE CURRENT DIRECTORY:

```
stud@comp:~> ssh stYYNN@std.academy.lv:62322
Password:                             // password is not displayed when entering
Last login: Thu Sep 21 11:08:13 2019
Have a lot of fun ...                 // authorization was successful
stYYNN@std:~> pwd                     // command input
/home/student                         // output results
stYYNN@std:~>                         // shell prompt
```

4.2.2. DEFINITION OF THE CURRENT DATE AND TIME:

```
stYYNN@std:~> date                    // command input
Mon Sep 16 14:29:00 EEST 2019         // output results
stYYNN@std:~>                         // shell prompt
```

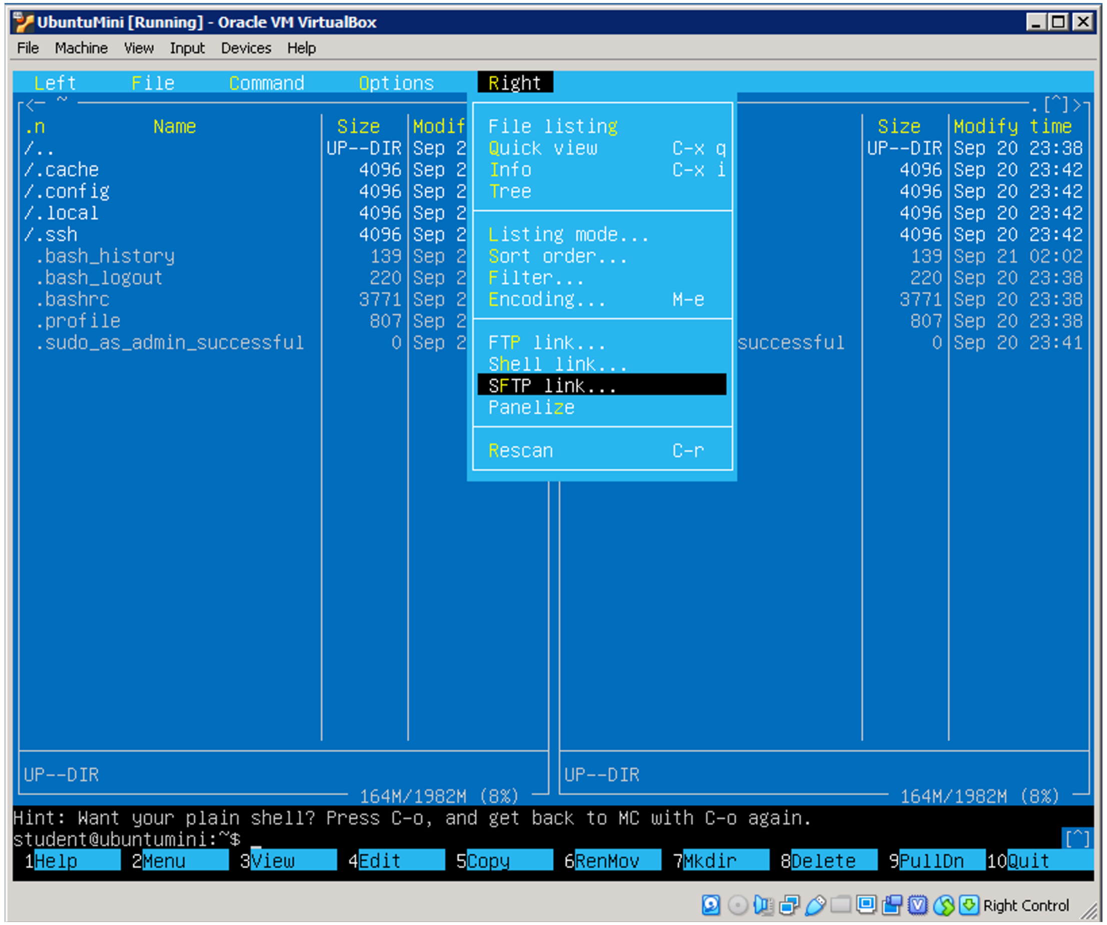
4.2.3. VIEW A LIST OF DIRECTORY FILES:

```
stYYNN@std:~> ls -ABl
total 212
-rw ------- 1 stYYNN users 782 Feb 20 12:33 .bash_history
-rw-r - r-- 1 stYYNN users 1177 Sep 27 13:49 .bashrc
drwx ------ 7 stYYNN nobody 4096 Oct 21 11:09 .beagle
drwxr-xr-x 2 stYYNN users 4096 Sep 27 13:49 bin
-rw-r - r-- 1 stYYNN nobody 26 Feb 20 04:20 description.txt
drwxr-xr-x 2 stYYNN nobody 4096 Oct 21 10:59 Desktop
-rw-r - r-- 1 stYYNN users 208 Sep 27 13:49 .dvipsrc
-rw-r - r-- 1 stYYNN users 1637 Sep 27 13:49 .emacs
```

4.2.4. COPY FILES WITH MIDNIGHT COMMANDER FILE MANAGER (MC)

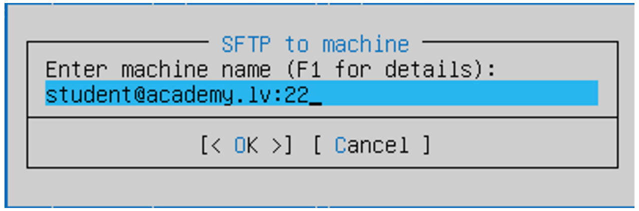
1. Start Midnight Commander on local Linux (command mc)

2. Configure SFTP connection to academy.lv remote server: F9 → Right → SFTP link … → stYYNN@std.academy.lv:62322 →Enter password



UbuntuMini [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Control

```
 Left     File     Command     Options    Right
┌<─ ~ ───────────────────────────────── ┌───────────────────────┐ ──────────────.[^]>┐
│.n          Name          │ Size │Modif│ File listing          │       │ Size │Modify time │
│/..                       │UP--DIR│Sep 2│ Quick view       C-x q│       │UP--DIR│Sep 20 23:38│
│/.cache                   │  4096│Sep 2│ Info             C-x i│       │  4096│Sep 20 23:42│
│/.config                  │  4096│Sep 2│ Tree                  │       │  4096│Sep 20 23:42│
│/.local                   │  4096│Sep 2├───────────────────────┤       │  4096│Sep 20 23:42│
│/.ssh                     │  4096│Sep 2│ Listing mode...       │       │  4096│Sep 20 23:42│
│ .bash_history            │   139│Sep 2│ Sort order...         │       │   139│Sep 21 02:02│
│ .bash_logout             │   220│Sep 2│ Filter...             │       │   220│Sep 20 23:38│
│ .bashrc                  │  3771│Sep 2│ Encoding...        M-e│       │  3771│Sep 20 23:38│
│ .profile                 │   807│Sep 2├───────────────────────┤       │   807│Sep 20 23:38│
│ .sudo_as_admin_successful│     0│Sep 2│ FTP link...           │successful│  0│Sep 20 23:41│
│                          │      │     │ Shell link...         │       │      │            │
│                          │      │     │ SFTP link...          │       │      │            │
│                          │      │     │ Panelize              │       │      │            │
│                          │      │     ├───────────────────────┤       │      │            │
│                          │      │     │ Rescan             C-r│       │      │            │
│                          │      │     └───────────────────────┘       │      │            │
├──────────────────────────────────────────┤├───────────────────────────────────────────┤
│UP--DIR                                   ││UP--DIR                                    │
└─────────────────── 164M/1982M (8%) ──────┘└──────────────────── 164M/1982M (8%) ──────┘
Hint: Want your plain shell? Press C-o, and get back to MC with C-o again.
student@ubuntumini:~$ _                                                               [^]
 1Help    2Menu    3View    4Edit    5Copy    6RenMov   7Mkdir   8Delete  9PullDn 10Quit
```



```
┌──────────── SFTP to machine ────────────┐
│ Enter machine name (F1 for details):    │
│ student@academy.lv:22_                  │
├─────────────────────────────────────────┤
│          [< OK >]  [ Cancel ]           │
└─────────────────────────────────────────┘
```

3. Copy any file from local Linux to remote server and back from remote to local.

4. Logout from mc for close remote SFTP connection (command exit or key [F10]).

4.2.5. Executing commands on a remote computer and without loading a remote shell

The ssh command can be used to execute commands on a remote computer and without loading the remote shell. In this case, the required command is passed as the ssh parameter: ssh <hostname> <command>

For example, if you want to execute the ls /usr/share/doc command on the remote academy.lv computer, at the shell prompt, enter:

```
stud@comp:~> ssh stYYNN@std.academy.lv:62322 ls /usr/share/doc
```

When you enter the correct password, the contents of /usr/share/doc will appear on the screen, and you will return to your shell prompt. It should be noted that not all commands can be executed in this way. An example of a failure when trying to start mc:

```
stud@comp:~> ssh stYYNN@std.academy.lv:62322 mc
Password:
Cannot get terminal settings: Invalid argument (22) // Error! Unable to get terminal settings
TERM environment variable needs set.
stud@comp:~>
```

4.2.6. Copy files with SCP command

To transfer files between computers over a secure connection, use the **scp** (secure copy) command.

a) To transfer a local file to a remote computer, this command is used in the form: **scp localfile username@tohostname:/newfilename**

In order to transfer the local somefile to academy.lv under student username, enter in the shell prompt (replacing student with your name):

```
stud@comp:~> scp somefile stYYNN@std.academy.lv:62322:/home/users/student
```

In this case, the local somefile file will be copied to /home/users/student/somefile on the academy.lv server.

b) To transfer the remote file to the local computer, use the scp in the form: **scp username@tohostname:/remote/file /new/local/file**

c) As source files several files can be specified. For example, to transfer the contents of the /downloads directory to an existing directory named uploads to the std.academy.lv remote computer, enter the following command at the shell prompt:

```
scp /downloads/* stYYNN@std.academy.lv:62322:/uploads/
```