GUIDELINES for Assignment 2 – Practical work 1 – task 2

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 practical work, 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-securit y
• 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

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

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.

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

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

– login name;

-ssh server name;

– port

number

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

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

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.

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:

-Definition of the current directory

-Definition of the current date and time

-View a list of directory files

Copy files with Midnight Commander file manager (mc)

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

2. Configure SMTP connection to academy.lv remote server: F9- RightS FTP link …

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])

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>

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:

Cannot get terminal settings: Invalid argument (22) // Error! Unable to get terminal settings TERM environment variable needs set

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

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.