ICT & Infra S2 M/S week 5: Secure network protocols, part A

**Class: I02**

**Student numbers:**

**Student names: Mihai Glodici**

Date: Feb 2020  
Version 1.2

# Introduction

In this exercise you will learn how to make a secure connection via SSH, copy files using SCP protocol and make remote connections without a password ( bonus, challenge ).

How to deliver your assignments?

Fill in this document with required information about your group. Answer questions and upload the document to Canvas at most one week after the assignment is given.

## *Assignment 1: Deploy a template of Debian or Lubuntu Linux machine and place this into your private VLAN.*

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-2_5.png. Estimated time: 45-60 minutes.

To deploy the Linux machine, you may use Seclab infrastructure of Fontys. Please refer to the manual “Working in a virtual environment”.

Login/password for Linux machine (also for administrator rights): “student”/”student”.

You do not need to provide any proofs to show successful deployment.

## *Assignment 2: SSH server*

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-2_5.png. Estimated time: 15 minutes.

Make sure OpenSSH server is installed on your Linux machine. It is installed by default on Linux machine from SecLab.

Otherwise run:

# sudo apt install openssh-server

From this moment your server wil listen to incoming SSH connections on port 22.

Look for the ip-adress on your linux machine:

# ifconfig

Provide a screenshot for installation of SSH server. A computer screen capture

Description automatically generated with medium confidence

## *Assigmnent 3: PuTTY ssh client*

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-3_5.png. Estimated time: 90 minutes.

Download and install ssh-client program PuTTY for windows http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

On your Windows machine (preferable in same network) you will see this GUI if you start PuTTY:



In this window you can choose between options to connect to the remote machine like Telnet, Rlogin, SSH, etc.

Which of these connection types are the safest? Telnet, Rlogin or SSH?

Explain which protocol and why.

 SSH (which stands for ‘secure shell’) is a recently designed, high-security protocol. It uses strong cryptography to protect your connection against eavesdropping, hijacking and other attacks. Telnet and Rlogin are both older protocols offering minimal security.

 SSH and Rlogin both allow you to log in to the server without having to type a password. (Rlogin's method of doing this is insecure, and can allow an attacker to access your account on the server. SSH's method is much more secure, and typically breaking the security requires the attacker to have gained access to your actual client machine.)

Source: https://documentation.help/PuTTY/which-one.html

## *Assignment 4: Test your SSH connection.*

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-3_5.png. Estimated time: 15 minutes.

Open your SSH client on your Windows/Linux client and connect to the ssh server on your SecLab VM machine.

# ssh <hostname of server>

(e.g. ssh 192.168.1.1, or ssh student@192.168.1.1 22)

Use the right credentials and you have a successful connection.

Show via command who (or just w) your connection.

Provide the output of command ‘who’. A computer screen capture

Description automatically generated with medium confidence

## *Assignment 5: Copy file to Linux machine.*

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-3_5.png. Estimated time: 15 minutes.

Research on internet how to copy a file from your Windows machine to a Linux machine using SCP protocol.

Provide a screenshot of the command syntax and the results of successful copy of a file.

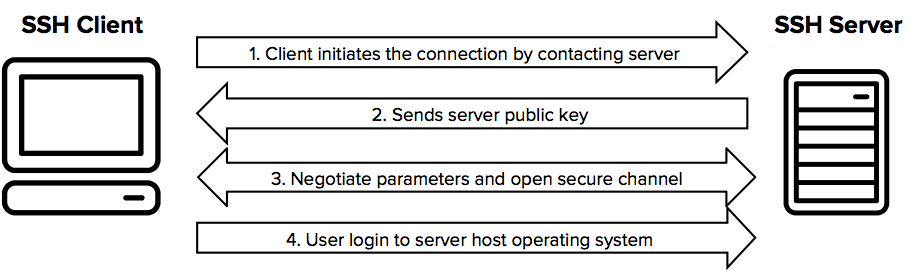
A screenshot of a computer

Description automatically generated with medium confidence

## *Assignment 6:* Wireshark study.

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-3_5.png. Estimated time: 60 minutes.

## Explain steps on the picture below in detail. Make screenshots of wireshark capture of all 4 steps of the process below.



To begin, a TCP connection is established between my computer and the VM using putty, using SYN, ACK packets.

Then it establishes a connection using the SSHv2 protocol.

The next stage is client-server key exchange initialization.

Following that, the real keys (Elliptic Curve Diffie-Hellman Keys) are exchanged between the client and server, and vice versa.

The username and password are then sent.

Graphical user interface, text, application

Description automatically generated

## *Bonus assignment 7: Investigate how to make SSH login without a password.*

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-3_5.png. Estimated time: 120 minutes.

Provide explanation, steps and necessary screenshots.