Lecturer
Prof. Dr. Christian Tschudin (christian.tschudin@unibas.ch)

Tutors
Carlos Andrés Tejera (carlos.tejera@stud.unibas.ch)
Andreas Wassmer (andreas.wassmer@unibas.ch)

Uploaded on
Thu., 17 March 2022

Deadline
Wed., 30 March 2022
Upload on ADAM

Task & Idea

In this exercise sheet, we start with some basic network operations and will train the handling of the secure shell and file exchange with remote targets.

For this exercise sheet, we expect you to hand-in written solutions as PDF and a partial presentation in a online meeting. Besides explanations and answers to questions, the PDF should contain the detailed documented source code and for tasks not to be presented (noted in the question) a list of all executed commands and generated outputs (as screenshots if relevant). The solutions can be handed-in in groups of two. The presentation will take place in the week of the deadline.

Exercise 1 - Network Basics Part I - Return to Sender... (1 Point)

You can use the Linux programs : `dig`, `ping`, `traceroute`, `whois` (see `netutils` package). For reference, we assume you to be located within the University network or to be connected via VPN to the network. Why is this relevant?

(a) Identify "https://switch.ch" : To identify this service, we require its IP , the owner and its location (if possible). Explain how you did that.

(b) Ring-Ring, is anyone home? Which ones of these addresses

informatik.unibas.ch
www.zurich.ibm.com
www.tik.ee.ethz.ch
www.amazon.com

can be pinged and which can be accessed via browser? Why?

Exercise 2 - Network Basics Part II - Around the World (1 Point)

You can use the Linux programs : `dig`, `ping`, `traceroute`, `whois` (see `netutils` package). Some additional helpful tools are

http://www.traceroute.org
http://www.yougetsignal.com/tools/network-location/

For reference, we assume you to be located within the University network or to be connected via VPN to the network. Why is this relevant?

i) What is the minimal and maximal Round-Trip-Time connecting to web.mit.edu and what is its dependency to its package size?

ii) How many Hops are between you and "Sheldon's Office" (tBBT)?

iii) Through which countries does the signal travel?

iv) Do the following connection targets share partial routes? (No detailed list, but test yourself and try to explain why.)

https://sandiego.edu
english.pku.edu.cn
univie.ac.at

Exercise 3 - Network Basics Part III - the Idle Overload of Network Traffic (1 Point)

(a) Hogging the network bandwidth : Assume a shared connection of $10\,MB/s$. Each user wants $2\,MB/s$ of bandwidth and uses it $35\,\%$ of the time.
How many users are supported without wait, or reduced bandwidth, each using *circuit switching* and *packet switching*? Is there a difference and why?

(b) The weak link : For a file transfer of exactly $2\,GB$ we assume a connection with the route $\rightarrow A \rightarrow B \rightarrow C \rightarrow D \rightarrow$. All proxies have the following network traffic limits :

$$\begin{gathered} A\,(7\,MB/s \text{ UP}, 7\,MB/s \text{ DN}) \,, \\ A\,(7\,MB/s \text{ UP}, 7\,MB/s \text{ DN}) \,, \\ B\,(4\,MB/s \text{ UP}, 5\,MB/s \text{ DN}) \,, \\ C\,(6\,MB/s \text{ UP}, 3\,MB/s \text{ DN}) \,, \\ D\,(512\,KB/s \text{ UP}, 1\,MB/s \text{ DN}) \,, \end{gathered}$$

and there is no other network traffic.

i) How long and with what average speed executes the file transmission?

ii) If additional network traffic occurs, which are the 4 types of delays that could impact on this transmission?

Exercise 4 - SSH Server-Setup and Handling - Basic Setup (2 Points)

The software tool SSH (Secure Shell) allows to securely connect devices in a network and encrypting communication and to log-in remotely. The encryption includes the authentication part of the communication, and supports different cryptographic methods. To move files, there exist several protocols, a very common one is sFTP (secure file transfer protocol) and his predecessor SCP (secure copy).
In a first step, common SSH tools shall be tested to get acquainted setting up and using basic password-based and encrypted authentication for secure encrypted communication. In a next step, a 3 node setup with 2 servers and 1 client shall be prepared to allow omni-directional communication between the nodes.
Use the 2 VMs from the previous exercise sheet, the your host OS as nodes to configure. This setup, plus optionally the nodes from your exercise-partner, shall be used for the following tasks and exercises.
Although you can freely choose the software for your SSH setup, we recommend :

- OpenSSH 8.8 as CLI interface (an older version will do as well for this basic setup) (Win/Unix) https://www.openssh.com/
- Putty , alternative CLI/GUI interface (Win/Unix) https://www.chiark.greenend.org.uk/ sgtatham/putty/
- Bitvise SSH , GUI interface incl. File-Transfer (Win) https://www.bitvise.com/
- WinSCP , GUI File-Transfer (multiple protocols) (Win) https://winscp.net/eng/index.php
- CyberDuck , less ideal for this exercise :
  GUI File-Transfer + Interface for Web-Storage-Provider (Win/Unix) https://cyberduck.io/

Remarks :

- The communication between devices on a network (virtual and otherwise) depends on the network and how it is connected!
- While working in the university, being connected with `Eduoam` (and especially `unibas-public`) does prevent you to directly access another client computer. (Servers like SciCore can be accessed). Keep in mind that you need a direct network-connection (e.g. Lan cable) to directly connect to an other computer.
- If you get stuck, there are steps for common setup, for which you can find many detailed instruction by web-search.

Tasks : Answer the following questions in writing and execute the steps. You only need to write down asked observations.

(a) Installation der SSH Library und CLI

- Install SSH server (plus library and client) on both VMs.
- Add SSH server to start automatically in the background even without manual login, i.e. local user login.
- Add a user account or modify an already existing non-root user account to be logged in via SSH.
  (Hint:...)
- Install SSH client on your host OS

(b) Test your configuration by logging in onto both VMs.

Exercise 5 - SSH Server-Setup and Handling - Expanding for Automatisation (4 Points)

Tasks : Answer the following questions in writing and execute the steps. You only need to write down asked observations. In a debriefing, you will show the final steps marked with (*).

(a) Try connecting and logging in from one VM to the other. Is any change in configuration necessary and why? (Depending on your setup.)
Retest your configuration and confirm the connection between both VMs in both directions.

(b) Switch login for all connections to ssh key-pair based login (Hint: Each connection needs a key-pair, with a key-part stored on either side. With password-based SSH you can already use sFTP or SCP to exchange files.)

(c) Store SSH connection configuration on both VMs (to connect to one another) and your host client.

(d) (*) test your sFTP or SCP connection by :

- Create a text-file on your host system.
- SCP/sFTP the text-file to either VM
- Rename the file with a RPC (remote procedure call) without actual/tranditinoal logging-in to the VMs
- SSH log-in to the VMs and edit the file(s).
- SCP/sFTP from the client to pull the file back.
- Directly copy the file(s) from either VM to the other. → `scp server1:/tmp/file1.txt server2:/tmp`
- Directly copy the file(s) from either VM to the other with flag "-3" and explain the difference. → `scp -3 server1:/tmp/file1.txt server2:/tmp`

Exercise 6 - Shark Infested Waters (2 Points)

Although you can freely choose the software for your SSH setup, we recommend :

- Wireshark , Comm-Analyser https://www.wireshark.org/
- X-servers :
  - Linux : part of the OS (Linux-GUI)
  - MacOS : xQuartz (https://www.xquartz.org/)
  - Windows : part of CygWin s(https://www.cygwin.com/)

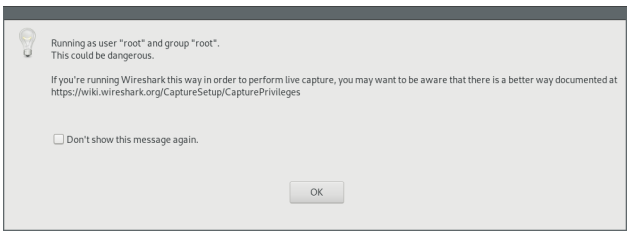
Tasks : Answer the following questions in writing and execute the steps. You only need to write down asked observations. In a debriefing, you will show the final steps marked with (*).

(a) Install Wireshark on your client and both VMs.

(b) (*) Because Wireshark is a GUI-based application, how does this work with a terminal-based system? Do the necessary steps to execute Wireshark on the terminal based VM. (Hint: In Linux the GUI is called X-system and is split into two parts, a client for the terminal side and a server for the GUI side, if not on the same machine. SSH supports X forwarding.)

Exercise 7 - Wireshark Capture Privileges (2 Punkte)

Wireshark enables you to analysis incoming and outgoing network packets without disturbing running applications. For this purpose, Wireshark taps the packets directly from the network card. This process requires superuser rights. However, if Wireshark is run with root privileges, you see the following warning message:



(a) Explain the issue that is pointed out in the warning message

(b) Configure your system so that you do not need to run Wireshark as `root` to record traffic (the warning shall no longer appear). If the packet manager of your operating system has already this configuration, investigate and explain this configuration.

Exercise 4 – Network Anaylsis with Wireshark (3 Punkte)

Copy files from `server1` to `server2` as tested in the preparations. In the meantime, record incoming and outgoing network packets from `client1` and `server2`. Examine the recorded traffic:

- Open Wireshark and start recording the packets on the active network interface
- Filter the output in Wireshark to show only packets sent to or from the other two systems.
- Filter further so that only SSH traffic is displayed.

How does `scp` differ with and without the -3 flag? On which route is the file transferred through the network?