# NS Lab 1 Assignment

## Network Tools

Fahimeh Alizadeh (f.alizadehmoghaddam@uva.nl)

Rex Valkering (rexvalkering@gmail.com)

Sam Ansmink (sam.ansmink@student.uva.nl)

Koen Koning (koenkoning@gmail.com)

Lab date: Oct. 27 & 30, 2014

Hand-in time (submit to blackboard) by Nov. 3, 2014 12:00CEST

Total points: 20 pts

**Abstract**

This assignment focuses on various useful network tools such as: Wireshark, iperf, ping, traceroute, netstat and nmap. Please have in mind that most of the exercises in this lab have to be done on a Linux machine. Therefore we strongly advise you to carry out this lab exercise on the lab Linux machines.

**Note**: You can find *iperf* and *nmap* at the following directories in the linux lab machines:

```
/opt/linux-x86_64/ict/iperf-2.0.4/bin/iperf
/opt/linux-x86_64/ict/nmap
```

If you have problem with the above installation then you can download the source codes and install them in your home directory. Have in mind that when you configure the installation, you have to define your home directory as the destination directory (`./configure --prefix=$HOME`). You can find the source codes from here:
http://sourceforge.net/projects/iperf/?source=dlp
http://nmap.org/download.html

## Task 1 – Application Layer

### Task 1a – Wireshark – HTTP

Please, before starting this task, read the lab1-appendix1 for more information on Wireshark.

Start the Wireshark program and next open the trace file *wireshark_trace_task1a* from the Assignment folder on Blackboard. This file includes the traffic when a local machine connected to the web server *www.w3.org* using the HTTP protocol. Answer the following questions.

**Questions:**

1. (a) What is the IP address of the *"ss64.com"* server? (b) What is the IP address of the source computer? (c) Which page did the source computer request from that server?

2. (a) How many HTTP GET message the source computer sent to the *"ss64.com"* server? (b) Which filter did you apply to give you only the HTTP GET messages towards the *"ss64.com"* server?

### Task 1b – Wireshark – Security

Start the Wireshark program and next open the trace file *wireshark_trace_task1b* from the Assignment folder on Blackboard. This file includes the traffic when the local machine connected to the web server *gaia.cs.umass.edu* using the HTTP protocol. Answer the following questions.

**Questions:**

3. (a) Determine the hostname from the IP address *"128.119.245.12"*? (b) What is the username? (c) What are the passwords sent by the user to the server? (d) Which one is the 'correct' password? (e) What is the message sent to the user in case of entering correct password?

### Task 1c – Command Line Tools: nmap, nc, curl, wget

Answer the following questions using command line tools. You can find more information about each command using the manual command (*man <tool_name>*).

**Questions:**

4. *Ping* the host *"www.ebay.com"*. (a) Do you get any response? Now try the tool *nmap*, (b) is the host up? (c) What ports are open? (d) What service is on each port?

5. Using the *nc* command, test that the server www.ebay.com is listening to port 80 from the port number 3130, without sending any data to the server (a) Give the exact command that you execute, (b) what is the result of the command: *"printf "GET / HTTP/1.0\r\n\r\n" | nc www.ebay.com 80"*?

6. The address space 192.16.191.0/24 is part of the CWI network. Using *nmap* find which hosts are up in this network. Find only the up hosts, with out scanning for open ports. (a) Give the exact command that you executed. (b) How many hosts are up?

7. Using the *nc* command create a basic server/client model. First create a server that listens to the port 3130. Then create a client that connects to the server. (a) What is the command that you typed for the server? (b) What is the command that you typed for the client? After the connection is established, type something at the server and next at the client console. (c) What is happening? (d) How could you stop the server from listening at the client console? *Hint: use the loopback: 127.0.0.1*

8. Using *curl* find all redirections of www.uva.nl. (a) What is the command that you typed? (b) List type and version of the webservers that serve www.uva.nl? Try also for www.google.com. (c) Do you get the type and version of the webserver? If not explain, why do you think this happen?

## Task 2 – Network Layer

### Task 2a – Wireshark - Investigate Traceroute

In this task you are going to investigate how traceroute works, using a Wireshark trace file. Please read the lab1-appendix2 for more information on traceroute.

Start the Wireshark and load the file *wireshark_trace_task2a.* In this file we captured the traffic generating by a traceroute command using ICMP packets. Answer the following question based on this trace file.

**Questions:**

9. (a) What is the IP address of the host that executed the command, and (b) What command is executed at the source host? (c) How many hops away is the target host?

10. The traceroute finds the path between a source and a target host. In the first step it finds the host/router that is one hop away, in the second step it finds the host that is two hops away and so on, until it reaches the target host. From the trace file, (a) find how many ICMP packets the source host was sending in each step? (b) How did you find that?

11. Explain, based on the trace file, how the ICMP traceroute works: (a) what type of messages does the source host send? (b) What type of messages does it receive from the intermediate host, each time? (c) How does it know that a sending packet reaches the target host?

**Task 2b – Ping and Traceroute - Find availability and RTT**

Using the tools ping and traceroute you are going to check the availability and RTT. Please read the lab1-appendix2 for more information on traceroute and ping.

```
www.cwi.nl
www.uva.nl
www.nikhef.nl
www.amazon.com
www.twitter.com
```

**Questions:**

12. Using the ping command find the availability of the above hosts. (a) Which hosts are available? For the hosts that are not available check if their websites are available. (b) Why do you think those hosts are not responding to the ping?

13. Using ping, calculate the mean RTT (round-trip time) for three packets, for the hosts. (a) Give the mean RTT for each one host. (b) Do all the hosts have the same or very close RTT times? (c) If not, explain why. (d) What type of packet-delay causes this difference?

14. Use the IPv4 traceroute program (from: http://www.ntua.gr/nmc/traceroute.html) for the hosts: *www.berkeley.edu* and *www.stanford.edu*. (a) In which part of the path towards the destination the biggest delay is introduced? (b) Explain why?

15. Execute two ping commands to *www.surfsara.nl*. For each ping command send exactly 10 packets. For the first one set the size of the packets to 32 bytes, and for the second one to 1024 bytes. (a) Give the exact commands that you executed. (b) What is the percentage of packet loss and (c) what is the average RTT in each case? (d) Is the average RTT different in each case? (e) If yes explain what type of packet-delay cause this difference?

**Task 2c – Traceroute - Find the network path**

**Questions:**

Perform IPv4 traceroute from a host in Greece (http://www.ntua.gr/nmc/traceroute.html) and in Hungary (http://diag.vh.hbone.hu/mtr/) to the host *www.surfnet.nl*.

16. (a) How many links are the same in the two traceroutes? (b) Which are the same (give the IPs)? Try to identify where the largest delays are introduced. (c) Can you explain where?

17. Perform a traceroute from a host in Greece (http://www.ntua.gr/nmc/traceroute.html) and in Hungary (http://diag.vh.hbone.hu/mtr/) to www.google.com. (a) How many links are the same in the two traceroute commands? (b) Explain why.

## Task 3 – Transport Layer

### Task 3a – Iperf

iperf is a tool for performing network throughput measurements. For more information check at: http://code.google.com/p/iperf/, or execute at command line: *man iperf*.

**Question:**

On the machine *rembrandt0.uva.netherlight.nl*, an iperf server is running, at the port 5001

18. From your machine execute an iperf command to check the bandwidth between your machine and the server. Check also the TCP Maximum Segment Size (MSS). (a) Give the exact command that you executed, (b) what is the bandwidth? (c) What is the MSS? (d) Are there any lost packets? If yes give the number. (e) Execute a ping command; what is the RTT between your host and the server?

19. The TCP window size field controls the flow of data, and before RFC 1323 its maximum value was 65KB. The iperf default value is 129KB. Execute iperf with different TCP window sizes (at least 10 times; set the window value in range from 5KB to 500KB). (a) Give the syntax of the command. (b) For each execution give the window and the throughput. (c) Which is the TCP windows size, which you find to have the best throughput?

### Task 3b – Netstat

With netstat command you can check the status of the network.

**Question:**

20. Execute a netstat command to display only UDP ports. (a) What is the exact command? (b) What UDP ports are currently used on your machine (write down 3)? Execute the netstat command to display only the TCP ports that are currently listening on your machine. (c) What is the exact command? (d) What TCP ports are currently used on your machine (write down 3)?

## Submission

You have to submit:

- Your answers to all the questions. Use the provided **answer sheet** for your answers and provide your answers in the appropriate answer field for each question.

- Answer only what each question ask, with out any superfluous details.

**Attention:** You have to submit **one PDF** file that contains all the answers; the name of the file should be ***lab1-<lastname_firstletter>.pdf*** *(example: lab1-alizadeh_f.pdf)*.

Any other kind of submission will not be taken into account. You must also put your full name and your student number at the top of the answer sheet.