NSS Lab 1 Assignment

Network Tools

Junchao Wang (J.Wang2@uva.nl)

Rex Valkering (r.a.valkering@uva.nl)

Daniël Louwrink (d.louwrink@uva.nl)

Daan Kruis (d.kruis@uva.nl)

Lab date: Sept. 7, 2016

Hand-in time (submit to blackboard) by Sept. 8, 2016 23:59 CEST

Total points: 10 pts

Abstract

This assignment focuses on various useful network tools such as: Wireshark, ping, traceroute and nmap.

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.iamsterdam.com* using the HTTP protocol. Answer the following questions.

Questions:

1. (a) What is the IP address of the "www.iamsterdam.com" server? (b) What is the IP address of the source computer? (c) Which packet firstly contains IP address of the "www.iamsterdam.com" server? Write down the number of the packet and the protocol type.

2. (a) How many HTTP GET messages has the source computer sent to "www.iamsterdam.com" server? (b) Which filter did you apply to give you only the HTTP GET messages towards the "www.iamsterdam.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 *www.gogo6.com* using the HTTP protocol. Answer the following questions.

Questions:

3. (a) Determine what did the host do with the www.gogo6.com? (b) What kind of information did the host send to the www.gogo6.com server? (c) Did the whole process go successfully?

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.reddit.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.reddit.com is listening to port 80 from the port number 4040, 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.reddit.com 80"*?
6. The address space 145.100.104.96/27 is part of the OS3 network. Using *nmap* find which hosts are up in this network. Find only the up hosts, without scanning for open ports. (a) What command did you use? (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 6060. Then create a client that connects to the server. (a) What command did you use for the server? (b) What command did you use for the client? After the connection is established, type something at the server and next at the client console. (c) What is happening?
8. Using curl find all redirections of www.twitch.tv. (a) What command did you use? (b) List the webservers that serve www.twitch.tv.

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. You can read more about traceroute in section 1.4.3 of the book and section 3.4 of RFC 2151 [ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt].

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 command is executed at the source host? (b) How many hops away is the target host? (c) How did you find that?
10. 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 sent 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.

www.bol.com
www.uva.nl
www.ns.nl
www.yahoo.com
www.alibaba.com
www.amazon.com

Questions:

11. 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?
12. Using ping, calculate the mean RTT (round-trip time) for three packets, for the hosts. (a) Give the mean RTT for each 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?
13. Use the IPv4 traceroute program (from: http://www.ntua.gr/nmc/traceroute.html) for the hosts: *www.yahoo.com* and *www.amazon.com*. (a) In which part of the path towards the destination is the biggest delay introduced? (b) Explain why.

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.ns.nl*.

14. (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?

15. 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.twitter.com. (a) How many links are the same in the two traceroute commands? (b) Explain why.

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 asks, without 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- Kruis_D.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.