Lab 1 – Networking Tools

Assistants

Johannes Blaser
Frederick Kreuk
Kyrian Maat
Niek van Noort
Cees Portegies
Zi Long Zhu

For questions email: nns18-tas@list.uva.nl

Lab dates

Tuesday 4 September

Deadline

Thursday 6 September at 23:59 CEST

Total points

10

This lab must be done individually

1. Abstract

This assignment serves as an introduction to various networking tools, some of which you will use in the online labs given during the remainder of the course. You will learn to capture and examine trace files in Wireshark, and to inspect the network using the command line utilities ping, traceroute, and nmap.

2. Preparation

Having Wireshark installed is essential for this lab. You can find the installation instructions at https://www.wireshark.org/download.html.

3. Submission

Hand in the answer sheet document filled in and saved as a PDF, with the following naming convention: `Lab1-<last_name>_<first_letter_of_first_name>.pdf`, for example `Lab1-Kreuk_F.pdf`.

4. Assignment

Monospaced fonts denote strings to be used literally in answering the question. Do not make any alterations, as this may cause you to find a wrong answer.

Task 1 – Application Layer

Task 1a – Wireshark

Before starting this task, read `NNS18-lab1-appendix1-wireshark.pdf` for more information on Wireshark.
Start the Wireshark program and next open the trace file `NNS18-lab1-task1a.pcapng` from the Assignment folder on Blackboard. This file includes the traffic from a local machine connected to the web server `lowendmac.com` using the HTTP protocol. Answer the following questions.

Questions:

1. (a) What is the IP address of the `lowendmac.com` server?
   (b) What is the IP address of the source computer?

(c) Which is the first packet to contain the IP address of the `lowendmac.com` server in the payload? Write down the number of the packet and the protocol type.

2. (a) How many HTTP GET messages has the source computer sent to the `lowendmac.com` server?
   (b) Which filter did you apply to give you only the HTTP GET messages towards the `lowendmac.com` server?

Task 1b – HTTP Authentication

In this task, you are going to examine a basic authentication system. The website to be examined is: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html . The website is password protected with the following login information; the username is "`wireshark-students`" and the password is "`network`".
To examine the authentication in the HTTP packets do the following:

- Clear the cache of your browser and restart it
- Start the Wireshark capture
- Go the URL: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
  When presented with the login popup, login with the previously mentioned login details
- Stop the Wireshark Capture

Based on this capture, answer the questions below.

Questions:

3. (a) What is the initial server response (status code and phrase) in response to the initial HTTP GET message from your browser?
   (b) When the second HTTP GET message is sent, what new field is included in the packet sent to the server?

Task 1c – More tools: nmap, netcat

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.surfspot.nl`
   (a) Do you get any response?
   (b) Now try the tool `nmap`, 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.cambridge.org` is listening on its port `80` when you are connecting from port number `4040`, without sending any data to the server.
   (a) Give the exact command that you used.
   (b) Describe the result of the command (do not copy the output):
   ```
   printf "GET / HTTP/1.0\r\n\r\n" | nc www.cambridge.org 80
   ```

6. The address space `145.100.104.96/27` is part of the OS3 network. Using `nmap`, find only the hosts that are up in this network 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 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?
   (c) After the connection is established, type something at the server and next at the client console. What is happening?

8. Using `curl`, find all redirections of `www.anandtech.com` .
   (a) What command did you use?
   (b) List the server software running on the machines that serve `www.anandtech.com` .

Task 2 – Network Layer

Task 2a – ICMP

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 Wireshark and load the file `NNS18-lab1-task2a.pcapng`. In this file, we captured the traffic generated by a traceroute command using ICMP packets. Answer the following questions based on this trace file.

Questions:

9. (a) What command is executed at the source host? Give the full command, including any flags and/or arguments.
   (b) For any flags and/or arguments used in the command, how did you determine they were used?
   (c) How many hops away is the target host?
   (d) 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? What changes between messages?
    (b) What type of messages does it receive from the intermediate host, each time?
    (c) How does it know that a sent packet has reached the target host?

Task 2b – Ping and Traceroute

Using the tools ping and traceroute you are going to verify the availability and RTT of the following websites:

```
www.netflix.com
www.gvb.nl
www.nintendo.co.jp
www.surf.nl
www.nos.nl
www.auone.jp
www.craigslist.com
www.alipay.com
```

Questions:

11. Using the `ping` command, find the availability of the above hosts. The UvA network might cause the results to be unreliable. For best results, verify on your home network.
    (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 each host.
    (a) Give the mean RTT for each host.
    (b) Do all the hosts have the same or very close RTT times? If not, explain why.
    (c) What type of packet delay causes this difference?

13. Use the IPv4 traceroute program (from: `http://traceroute.insode.de/`) for the hosts: `www.surf.nl` and `www.craigslist.com`.
    In the path towards the destinations you can see ‘sudden’ increases in delay introduced. Focus on the largest increase in both paths. Where and why do these occur?

Task 2c – Tracerouting Network Paths

In the following questions you will perform IPv4 traceroutes from a host in the Czech Republic (http://lg.silesnet.net/) and in Poland (http://piotrkosoft.net/traceroute.php) to different hosts.

Questions:

14. Perform IPv4 traceroutes from both hosts to the host `www.buienradar.nl`
    (a) How many links are the same in the two traceroutes?
    (b) Which are the same (give the IP addresses and full hostnames)?
    (c) Explain what these links in the network are and why they are the same.
    (d) Try to identify where the largest increases in delay are introduced in both paths. If there are multiple increases of comparable size, mention them all. Try to explain why these increases occur specifically at these points.

15. Perform IPv4 traceroutes from both hosts to the host `pandora.com`
    (a) How many links are (approximately) the same in the two traceroutes?
    (b) Explain why these links are the same.

    Standard traceroutes do not always accurately and unambiguously reflect the paths taken by packets and can even result in paths that appear bizarre at first glance. It is often possible to notice these anomalies without knowing the true configuration of the network.
    (c) Find an anomaly that exists in both traceroutes you just performed. Explaining the cause of the anomaly is not required.