NS Lab 1 - Answer Sheet
Network Tools

Student Name: Sander
Student Surname: In 't Veld
Student Number: 10277935

Chariklis Pittaras (c.pittaras@uva.nl)

Karel van der Veldt (karel.vd.veldt@uva.nl)

Lab date: Sep 02 & 05 2013

Hand-in time (submit to blackboard) by Sep 9, 2013 13:00CEST

Total points: 20 pts

Please provide your answer in the appropriate space for each question

Task 1 – Application Layer

Task 1a – Wireshark – HTTP

1. (a) 128.30.52.37
   (b) 145.100.135.221
   (c) www.w3.org/Protocols/rfc2616/rfc2616.html

2. (a) 1.
   (b) http.request && ip.addr==128.30.52.37

Task 1b – Wireshark – Security

3. (a) 128.119.245.12
   (b) 'letsTry' and 'network'.
   (c) 'wireshark-students'.
   (d) http && ip.addr==128.119.245.12
   (e) 'network'.

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

4. (a) No.
   (b) Yes.
   (c) 80 and 443.
   (d) HTTP and HTTPS respectively.

5. (a) 'nc -z -v www.amazon.com 80'
   (b) “Connection to www.amazon.com 80 port [tcp/http] succeeded!”

6. (a) 'nmap -sP 192.16.191.0/24'
   (b) 8.

7. (a) 'nc -l 127.0.0.1 1234'.
   (b) 'nc 127.0.0.1 1234'.
   (c) Messages typed at the server appear at the client, and vice versa (i.e. we have established a method of communication).

8. (a) Apache Server
   (b) 2.2.3 (Red Hat)
   (c) The google site runs on Google Web Servers (“gws”), but no version information is available since they develop their own servers internally.

Task 2 – Network Layer

Task 2a – Wireshark - Investigate Traceroute

9. (a) 145.100.135.221
   (b) 192.16.191.44
   (c) 4 hops away.

10. (a) Two ICMP messages are sent for each hop.
    (b) Looking at the ICMP's.

11. (a) Type 8: echo requests.
    (b) Type 11: time-to-live exceeded.
    (c) He gets an echo reply (type 9) back.

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

12. (a) www.mit.edu, www.nikhef.nl, www.uoa.gr and www.twitter.com respond.
    (b) To avoid ping flooding.

13. (a) *twitter*: 115ms, *uoa*: 87ms, *nikhef*: 16ms.
    (b) Not at all.

(c) Twitter is based in the USA, the University of Athens is in Greece and NIKHEF in Amsterdam.
(d) Twitter and UOA have higher propagation delay due to the large distances between Amsterdam and the USA / Greece respectively. Twitter might also have higher queue delay, since it is a very popular service.

14. (a) The last few hops.
    (b) They are the largest hops, from the IPX at Amsterdam to one in the USA.

15. (a) *24bytes packet size:* 'ping -s 24 -c 10 www.nikhef.nl'.
        800bytes packet size: 'ping -s 800 -c 10 www.nikhef.nl'.
    (b) 0% in both cases.
    (c) 18ms and 25ms respectively.
    (d) Yes, significantly.
    (e) Transmission delay increases if the packet size is larger than the bandwidth at a certain choke point.

Task 2c – Traceroute - Find the network path

16. (a) Only the last two.
    (b) 145.145.19.170 and 145.0.2.10
    (c) Where the packets goes from IPX to IPX, such as FR->UK->NL in the first traceroute and Sydney->Telstraglobal->Amsterdam in the second traceroute.

17. (a) None.
    (b) Google has multiple servers spread across the globe, including in Switzerland and Australia.

Task 3 – Transport Layer

Task 3a – Iperf

18. (a) 'iperf -c rembrandt0.uva.netherlight.nl -p 5001 -m'
    (b) 873 Kbits/sec
    (c) 1448 bytes
    (d) No.
    (e) Approximately 100ms on average.

19. (a) I ran the bash script given below; oddly, Linux always doubled the request (therefore my arguments range from 2.5K to 250K).
    (b) See the results below.
    (c) A TCP window size of around 20Kbytes seems to give the best throughput.

```
for ARG in {“2.5K”, "5K", "10K", "15K", "25K", "50K", "100K", "150K", "200K", "250K"}
do
  iperf -c rembrandt0.uva.netherlight.nl -p 5001 -m -w $ARG
done
```

[ARG: TCP Window Size, Bandwidthin Kbits/sec]
2.5K: 5K, 443
5K: 10K, 635
10K: 20K, 806
15K: 30K, 802
25K: 50K, 805
50K: 100K, 854
100K: 200K, 845
150K: 300K, 824
200K: 400K, 831
250K: *416K*, 822

Task 3b – Netstat

20. (a) netstat -at
    (b) 56262, 55810, 44417
    (c) http, xmpp-client

Submission

You have to submit:

- Your answers to all the questions. Use this **answer sheet** for you 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-vanderveldt_k.pdf, or lab1-pittaras_c.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 file