SOLUTION

CIS 3329
Assignment 2

50 points

due: February 6, 2018

1. From your home computer answer the following questions. On Windows operating systems, use the `ipconfig /all` command. If you're using an Apple or *nix box, use the command `ifconfig`.

   (a) What's the physical (aka MAC) address of one of the interfaces on your computer?

   (a) n/a

   (b) What's the IP address?

   (b) n/a

   (c) Is the IP address that you've listed a public routable IP address or is it a private address behind a NAT? What is the private IP address range and what is the purpose of this type of address? You can find the answer to this in RFC 1918.

   n/a

   (d) Provide a link to RFC 1918

   https://tools.ietf.org/html/rfc1918

   (e) What are the DNS servers[1]?

   155.247.225.230

   (e) 155.247.225.231

   (f) What's the IP address of the default gateway?

   (f) 129.32.93.129

[1] If you're using a Mac or Linux box, you'd find this in the file `/etc/resolv.conf`.

2. Using an internet speed test, for example, like the one at DSLReports (http://www.dslreports.com/tools), or one provided by your ISP, test the speed of your home's internet connection. What is your upload and download speed?

2. _____

3. What is the contact information for the network operator of the temple.edu domain? This can be found by using a WHOIS service.

Enterprise Systems Group
Temple University Computer Services
7th Floor Wachman Hall
1805 N. BroadStreet
Philadelphia, PA 19122
UNITES STATES
215 204 5555
whois@temple.edu

4. Using traceroute[2] from your home computer, trace the path from your home to stat.elcat.kg.

   (a) What are some of the major cities that are on the path?

Philadelphia
New York City
Amsterdam
Frankfurt

   (b) In the path, can you find your public IP address? If you dont have a home router-firewall, it is likely the IP address on the first line of the tracert output. Otherwise, it's probably the address on the next line. (If you're behind a home router-firewall, you can cheat to find out your public IP address by going to a website like http://checkip.dyndns.org or http://www.whatismyip.com)

(b) n/a

   (c) In a web browser, go to the page http://stat.elcat.kg/trace.cgi, and do a trace back to your home public IP address. Is the list on the path exactly the reverse of the path that you found in the last question? If it isn't, why do you suppose that this might be?

n/a

[2] on Windows operating systems, the command is typed `tracert`

5. DNS

   (a) What are some IP addresses for gmail.com?

   172.217.2.5

   216.58.197

   (b) What are the name servers for drexel.edu?

   noc2.drexel.edu

   noc.drexel.edu

   (c) What is the mail server for temple.edu?

   (c) Google GMail

6. Enter your public home IP address into an online address location tool (e.g., Geobytes.com). How accurate were the results? How do you suppose such an address location tool might work?

   n/a

7. What kind of impact does the high-level structure of the internet (e.g. tier-x ISPs) have on the ability of an ISP to provide a certain quality of service for a particular class of data? For example, is it easy for my ISP guarantee that all of my VoIP traffic will get a low delay, and why?

   Difficult for ISP to guarantee a low delay, your internet provider cannot guarantee bandwidth as it's shared across all customers and has arrangements with other ISPs.

8. Home wireless

   (a) Do you have a home wireless access point?

   (a) n/a

   If your answer to part (a) is no, pick a wireless access point online and look up its specifications to answer the remaining questions.

   (b) Which wireless standard does if follow?

   (b) n/a

   (c) What is the maximum bit rate of this wireless standard?

   (c) n/a

(d) How does this compare with the bit rate of your home's connection to the Internet through your ISP?

n/a

(e) What is the approximate range of the signal of your home wireless access point?

n/a

(f) Which wireless encryption technologies are available on the access point? Which do you have enabled?

n/a

(g) What is an SSID (note that we're not asking for your access point's SSID, rather, we're asking about SSID's in general)? How does turning off SSID broadcast affect the security of your home network? Is this foolproof? Why or why not?

An SSID stands for Service Set Identifier, it is the "network name" helps you identify the desired network when there are multiple networks are operating in the same physical area. Turning off the SSID and not broadcasting the name of your network can prevent any unwanted access to your network from average "neighbors". Hackers will still be able to locate the network