CIS 457 – Fall 2018
Lab 02: Network Troubleshooting and Performance Measurement Tools

Due by: 9/18/18
Total Points: 25 Points **Submission format:** hardcopy (one report per group of 2 students)

Lab Objectives:

The purpose of this lab is to:

- Practice the use of RFC (Request For Comments), as a mechanism to propose and discuss new Internet protocols.
- Be familiar with different networking tools.

What to turn in?

- Answer to the following questions as well as screen shots as directed.
- In your lab report, organize and answer the questions by labeling each section with the same headings such as listed in the lab assignment (ex: **Question 1: ipconfig** ……..etc)
- In each section, list the question in BOLD first then list its answer second in non-bold format (ex: **Record ALL of your host's IP information.** …. etc)
- Note that the lab report will be returned ungraded if the lab report is submitted without complying with the above mentioned requirements.

Note:

- Commands format and options are written assuming the use of Linux system. If you plan to use a Windows system, make sure to use the alternative correct options.

Question 1: ifconfig (2 points)

ifconfig (for Linux/Unix) is among the most useful utilities in your host, especially for debugging network issues. *ifconfig* can be used to show your current IP information, including your address, and adapter type and so on.

a) Record your host's IP address information by entering *ifconfig* into a new terminal (your ip add starts with 35).

Question 2: nslookup

(3 points)

It is a tool used for resolving domain names and ip addresses.

1. Open a terminal and use the nslookup command to identify the IP address of www.psu.edu
2. Open a terminal and use the nslookup command to identify the host name associated with the IP address: 128.118.146.130

Note:
If nslookup command timed out for any reason, you may use the web based version of nslookup posted @ this link http://www.zoneedit.com/lookup.html use the "**DNS Lookup**" section.

Question 3: ping (5 points)

Read the RFC1739 page (ping tool section) @ http://www.rfc-editor.org/ and answer the following questions (you may familiarize yourself with these ping examples posted on this link first: http://www.thegeekstuff.com/2009/11/ping-tutorial-13-effective-ping-command-examples/):

Note that to stop ping from working → Hit (CTRL and C)

a) What kind of packet/message does ping send to the target (protocol creating this message)?
b) What kind of packet/message is sent back target (protocol creating this message)?
c) What is TTL parameter?
d) What is the ping's packet loss rate when you issue a ping from your computer to www.y.com ?
e) What is the –t option used for? Then ping the following sites using the command
    - Ping –t 2 psu.edu

- Ping –t 5 psu.edu
- Ping –t 10 psu.edu
- Ping –t 20 psu.edu

In each trial, explain the ping output in your lab report.

Now we want to ping some sites around the world to get an idea of what kind of round trip times we experience to different locations. Ping the following sites:

www.uu.se - University of Uppsala in Sweden
www.shanghai.gov.cn - Shanghai China

f) For each site, explain the ping output. Also record the ttl value(s) reported for each echo response packet.

Question 4: Traceroute Utility **(5 points)**

Traceroute utility is used to find out how a packet is routed to a certain destination. The output is a list of the routers through which the packet traveled to reach its destination with some statistics on how long packets take to reach that router.

Assume that you are the network admin for the CIS School at Grand Valley State University. The CIS School has a partnership with the Department of Computer Systems, Information Technology in Uppsala University. The CIS school faculty access Swedish students' records by sending their quires to students' info systems hosted at the Uppsala University in Sweden. CIS Faculty and staff expressed a concern about a significant amount of delay that their queries take. You decide to investigate the packets' response time from Allendale Campus to the Uppsala University using the Traceroute Utility.

a) How does traceroute get each router to respond to it?

Do a traceroute for the following site: http://www.uu.se

b) Then attach a screen capture for the output with your lab report. (here is the command to use traceroute www.uu.se in a new terminal)
c) Record the response time to get to the Uppsala University.
d) What could be the reasons for the long delay problem and what do you suggest solving it?

Question 5: Whois **(5 Points)**

OK, so we've used nslookup to identify the address of a host by its name, and used ping to determine whether that host is open for business, and used traceroute to figure out how we get there. Now, how can we tell who that host belongs to? The answer is to use whois utility.

The *whois* utility can be used to find out something about the organization that is responsible for a particular domain name and its network. The information an organization submits when they register the domain name is supposed to be posted on one of the whois servers. It is a crude way of finding out where sites listed in trace route are. It is not reliable since the only geographical information listed is the address of the contact person. For a large nationwide network this is not useful information to locate the specific routers you went through but for regional networks or specific sites it can at least pin down the general vicinity.

You can access the whois DB by opening a terminal and issue the command whois psu.edu to determine who that PSU domain belongs to?

- Describe how an attacker can use whois databases and the nslookup tool to perform reconnaissance on an institution before launching an attack.

Question 6 **(5 Points)**

Assume that you received a spam message such as shown in the figure below. Using the above mentioned networking tools, develop a step by step methodology to determine the spammer's info, domain to which the spammer's computer belongs to, and the contact info for this domain. **Show** the **output** for the step by step process that you developed to solve this problem. Also, attach a **screenshot** for all the commands' output that you used to solve this problem.

From: Johnson,Austin Todd
Sent: Saturday, September 9, 2018 9:53 PM
To: elsaidm@gvsu.edu
Subject: Your Email

Your Email was accessed from a different Country IP & will be suspended if not validated within 24hrs after receiving this email. Click *HERE* and fill the details to validate your IP.

IT DESK ©

Copyright © 2018 Mail! Inc

References:

1. http://www.rfc-editor.org/