**Lab 1 RFC and Networking Tools CS 457**

**Due by:** Jan. 21/10 **Total Points: 100 Points Submit through Blackboard**

**Lab Objective**The purpose of this lab is to:

* Learn about the well-known networking services,
* Practice the use of RFC (Request For Comments), as a mechanism for learning about Internet protocols.
* Be familiar with different networking tools

**Introduction**

The transport protocols in the TCP/IP protocol suite are TCP and UDP. These protocols identify applications that use them by means of port numbers. A port number is a 16 bit integer so the range of possible values is 0 - 65535. The port number range 0-1023 is reserved for standard services and these numbers are known as *well known numbers*. The use of well known numbers is maintained by the Internet Assigned Numbers Authority (IANA) now part of the Internet Corporation for Assigned Names and Numbers (ICANN).

There are many well-known network services provided by operating systems to serve the people who use networks. For example, on UNIX these services are listed in the file /etc/services. These services provide convenient ways to access system information. Unfortunately the services may be a drain on the system resources and some of them are a potential security hole for the system, so many system administrators decide to close many of the non-essential services.

**Directions for Preparing Lab Report.**

Start a text document with the following heading:

CS 457, Lab 1 Your Name Here

Jan. 21 / 2010

Then on that document type your answers to each question. Submit the completed document in paper.

**Question1 RFCs and Organization of the Internet (10 points)**

Point your web browser to <http://www.rfc-editor.org/>. Read the introduction page to get an idea what RFCs are about. At the end of the paragraph about RFCs there is a link to the IETF home page. Click on that link and then click on the Overview of the IETF link. Read the first section and answer parts a) and b). Now go back to the RFC editor home page. In the section describing the RFC Editor there is a link to an RFC Tutorial. Click on that link and read the first 13 slides. Use that information to answer parts a) through d).

1. Describe the roles of the following organizations: IETF, IESG, IAB and ISOC.
2. Who does the actual work of the IESG?
3. When did RFCs start and who was the first editor?
4. Describe the three tracks into which RFCs are organized.

**Question 2 (5 points)**

Then read the descriptions of three specific services, daytime, finger and the time protocol. For the daytime service, look for RFC0867, for the finger service, look for RFC1288, and for the time protocol, look for RFC0868. If you use the search tool on the RFCeditor site, you may have to use the phrase time protocol instead of simply time, and then answer the following questions:

1. Briefly, describe each of the above mentioned application protocols.
2. Does each application protocol use a specific port number to communicate on, if yes what is it?
3. What transport protocol does daytime, finger and the time protocols use?

**Question 3**

**Nslookup (10 points)**

nslookup is a tool used for resolving domain names and ip addresses. If you give it an ip address it will do a dns lookup and attempt to return the domain name. If you give it a domain name it will do what is called a reverse dns look up and attempt to give you the ip address of that host. The command is simply nslookup domainname or nslookup ipaddress.

1. Use nslookup to identify the IP address of www.uni-bremen.de
2. Use nslookup to find the domain name of 200.12.180.5

**Question 4 (30 points)**

**Ping.**

Before starting on the ping exercise, make sure your computer is able to receive ping requests. Next, you need to know the ip address of your computer. Open a command prompt window and type the command *ipconfig* and make note of the ip address of your computer. Type ping immediately followed by <Enter> and read the help display that results. Also google *ping man pages* and read the description there. Use this information to answer the following questions:

1. What kind of packet does ping send to the target?
2. What kind of packet is sent back?
3. What is TTL?
4. What is the –i option for(on Windows systems)? Then ping the following sites using the command

* Ping –i 5 www.cis.gvsu.edu
* Ping –i 15 www.cis.gvsu.edu

1. Ping the following sites in the order given. Each time if the ping succeeded, write down the ***only the summary statistics*** given at the end of the report. If the ping failed write down the reason given.
   1. localhost
   2. your neighbor
   3. The default gateway: 148.61.112.254
   4. An EOS machine: 148.61.162.120
   5. Grand Valley’s web server: www.gvsu.edu
2. List at least 3 possible reasons for getting a host unreachable result when you ping another host.

**Question 5 (25 points)**

**Traceroute**

The traceroute utility is used to find out how a packet is routed to a 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. On a Windows system the command is *tracert*. For practice do *tracert www.uio.no* which will trace the route to the University of Oslo’s web server. You might want to capture the window and paste it into a Wordpad document for future reference.

1. Do traceroutes for the following sites: www.uni-bremen.de, www.uu.se , www.vuw.ac.nz

Examine the domain names of the routers in the path. The next to the last element, the one just before the top level domain such as edu, net or com, is the domain name of the organization to which the router belongs. In the case of country domains, there may be a second level domain such as ac or edu above the organization domain. vuw.ac.nz is an example of that. For each of the routes traced, write down the *sequence of domains* through which the route passes. See example, below. If a router only reports its ip address, write that down.

For destination www.uio.no the route goes through domains gvsu.edu, mich.net, internet2.edu, geant2.net, nordu.net, uninett.no, uio.no

**Warning!** You may have to stop the traceroute process using ctrl-C. Give it about a minute to complete.

**Question 6 (20 Points)**

**Whois**

OK, so we've used [nslookup](http://www.rickconner.net/spamweb/tools.html#nslookup#nslookup) to identify the address of a host by its name, and used [ping](http://www.rickconner.net/spamweb/tools.html#ping#ping) to determine whether that host is open for business, and used [traceroute](http://www.rickconner.net/spamweb/tools.html#traceroute#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 nation wide 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. For the following questions you can either use the web site [www.networksolutions.com/**whois**/index.jsp](http://www.networksolutions.com/whois/index.jsp) or log in to an eos machine and use the whois service on eos. To do this open up a terminal window and use the command whois followed by a domain name or ip address.

1. Who owns the domain wsu.edu?
2. Determine the range of addresses used by gvsu.edu. Hint: Do an IP address lookup for any gvsu host address.
3. Describe how an attacker can use the tools we have looked at today to perform reconnaissance on an institution before launching an attack.
4. In your traceroute reports some routers only reported their ip addresses, not their domain names. Use whois and see if you can find out the domain one of those routers belongs to.