**COMP2410 2013 final exam paper**

**Australian National University**

**First Semester Examination - June 2013**

**COMP2410 Networked Information Systems**

|  |  |
| --- | --- |
| **Maximum marks:** | **60** |
| **Weight:** | **60% of the total marks for the course** |
| **Time allowed:** | **3 hours 15 minutes** |
| **Permitted materials:** | **None** |

Answer all questions.

Be precise. Avoid long-winded answers. Indicate clearly the question and part to which you are providing an answer.

There are five questions. All answers are to be submitted in plain text files found in directories named Q1 through Q5 in your home directory. You will need to enter the answers using an editor. Please remember to save the answers in the appropriate file. Save your changes frequently, so that you do not lose your work. Do not change the names of the directories or of the files.

The text files in each directory have question numbers entered in them already, so all you need to do is to write your answer alongside the appropriate question number. Leave at least one blank line between answers.

Good luck!!!

**Question 1 [10 marks]  
Directory: Q1  
File: Q1.txt**

Answer all questions. Each question is worth 1 mark.

1. Give the full name of an application layer protocol that uses TCP as the transport layer protocol.
2. State two advantages of Network Standards.
3. State two advantages of using Software As a Service (SaaS), with respect to cloud computing.
4. State two uses of cookies.
5. The default port number for SMTP is:

80   110   25   143

1. Briefly describe two situations where you might use wireless LANs.
2. Given the IPv4 address 192.168.1.12/28, what is its subnet mask?

255.255.255.255   255.255.255.0   255.255.255.240   255.255.255.192   255.255.255.128

1. In the context of computer security, a denial of service attack is an example of:

a passive attack    an active attack

1. What is the domain name and IPv6 address of an authoritative name server for australia.gov.au?
2. When Tom signs a message using RSA and sends it to Mary, which which key does he use for signing?

Tom's public key    Mary's public key    Tom's private key    Mary's private key

**Question 2 [15 marks]  
Directory: Q2  
File: Q2.txt**

1. Briefly explain how persistent connections and pipelining can help improve HTTP performance. [3 marks]
2. What are the advantages and security issues of Near Field Communication (NFC)? Briefly describe three application areas of NFC. [3 marks]
3. What is NAT? Looking at the figure given below, assume that a browser on client1.anu.edu.au is trying to fetch a web page fromoriginserver.com, with port numbers as shown. What does the NAT box do to packets going from client1.anu.edu.au tooriginserver.com? How do packets sent in response from originserver.com reach client1.anu.edu.au? [4 marks]
4. Bob and Tom both want to sign a contract and send it confidentially to Alice. They work in different locations, but have access to the Internet. Describe how they would go about doing this using public key cryptography, as a sequence of steps. How will Alice verify the signatures on the signed contract? [5 marks]

**Question 3 [15 marks]  
Directory: Q3  
File:Q3.txt**

1. Explain the key features of peer-to-peer (P2P) architecture, clearly distinguishing it from client-server architecture. [3 marks]
2. Briefly describe three kinds of mobile devices, and three kinds of wireless communications technologies. Include in your descriptions explanations of the differences among the different categories. [3 marks]
3. Define the key concepts underlying the conventional IT security model. [3 marks]
4. Identify three threat-vulnerability combinations that affect payments using mobile-phones, and safeguards that can be used to address those risks. [3 marks]
5. In the context of Malware, what do the terms 'vector' and 'payload' refer to? Include examples of each. [3 marks]

**Question 4 [5 marks]  
Directory: Q4  
File: Q4.txt**

OzU is a (hypothetical) Australian university. Imagine you are employed as a team member to upgrade the IT system. Management has decided to use a "cloud" service offered by the company SoftMili, to provide all staff and students with free email and web hosting using their servers located in the People's Republic of Nil (PRN). In testing the new service you see access by a user ID reported to be from the PRN Secret Police. You report to supervisor that the PRN government may be hacking the system to read staff and student data. But your supervisor explains that the university has a contract with SoftMili guaranteeing data privacy and the university lawyers confirm this meets Australian privacy law. Your supervisor tells you that you have misinterpreted the logs, there is no security risk and you are to put the system into production. What should you do?

To help you, here is a condensed extract of the ACS Code of Ethics:

1. The Primacy of the Public Interest: You will place the interests of the public above those of personal, business or sectional interests.
2. The Enhancement of Quality of Life: You will strive to enhance the quality of life of those affected by your work.
3. Honesty: You will be honest in your representation of skills, knowledge, services and products.
4. Competence: You will work competently and diligently for your stakeholders.
5. Professional Development: You will enhance your own professional development, and that of your colleagues and staff.
6. Professionalism: You will enhance the integrity of the Society and the respect of its members for each other.

Answer the following question:

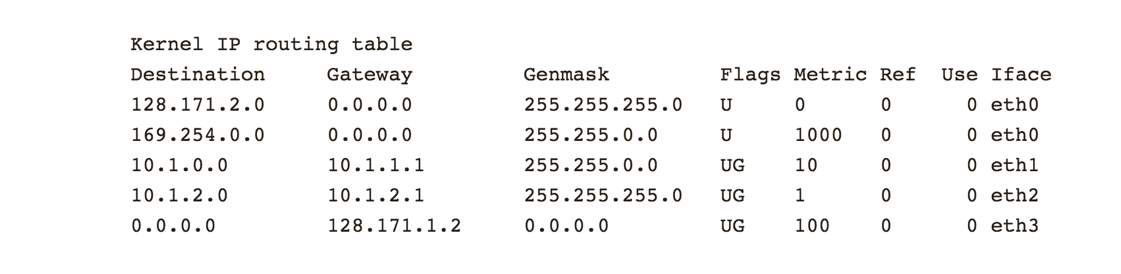
Describe two possible courses of action and the effects of these courses of action on yourself and others. Detail which values in the code of ethics would be relevant in deciding the course of action and why.

**Question 5 [15 marks]  
Directory: Q5**

**Question 5a [5 marks]  
File:Q5a.txt**

* 1. Determine the IP address and MAC address of your machine. What command(s) did you use to find the IP address? Include the output of the command(s) in your answer. [2 marks]

1. You are given the following output of the command 'route -n':



Assume that the machine that this command is run on has IP address 128.171.2.220. Answer the following questions. Each question is worth 1 mark. [3 marks]

* 1. Which interface will be used to send a packet to 128.171.2.126? Which router will be used?
  2. Which interface will be used to send a packet to 10.1.2.12? Which router will be used?
  3. Which interface will be used to send a packet to 128.171.20.63? Which router will be used?

**Question 5b [10 marks]  
File:Q5b.txt**

Using wireshark, load the file [tcpdump.out](https://wattlecourses.anu.edu.au/tcpdump.out). This is a tcpdump of a page fetch from www.google.com.au. Only look at the entries from 4-33. Answer the following questions:

1. Why are there 4 DNS related entries at the top? [1 mark]
2. What is the IPv6 address of www.google.com.au? Which are the authoritative name servers for this domain (give the domain names and IPv4 addresses)? [2 marks]
3. What do the entries 8-10 signify? [1 mark]
4. Explain the sequence of entries from 11-31? [3 marks]
5. What do the entries 32-33 represent? [1 mark]
6. What are the ethernet addresses of the two machines involved in the HTTP request/response? [1 mark]
7. What is the size of the page fetched, in bytes? [1 mark]