



**INTERNATIONAL ADVANCED DIPLOMA
IN
COMPUTER STUDIES**



**MODULE:
INTERNET SECURITY**

**ASSIGNMENT TITLE:
INTERNET SECURITY**

DECEMBER 2009

Important Notes:

- ❖ Please refer to the Assignment Presentation Requirements for advice on how to set out your assignment. These can be found on the NCC Education *Campus*. Scroll down the left hand side of the screen until you reach Personal Support. Click on this, and then on Policies and Advice. You will find the Assignment Presentation Requirements under the Advice section.
- ❖ You must familiarise yourself with the NCC Education Academic Dishonesty and Plagiarism Policy and ensure that you acknowledge all the sources which you use in your work. The policy is available on *Campus*. Follow the instructions above, but click on Policies rather than Advice.
- ❖ You must complete the ‘**Statement and Confirmation of Own Work**’. The form is available on the Policies section of *Campus*. Scroll down the left hand side until you reach Personal Support. Click on this and then click on Policies and Advice.
- ❖ Please make a note of the recommended word count. You could lose marks if you write 10% more or less than this.
- ❖ You must submit a paper copy and digital copy (on disk or similarly acceptable medium). Media containing viruses, or media which cannot be run directly, will result in a fail grade being awarded for this module.
- ❖ All electronic media will be checked for plagiarism.

Marker's comments:

Moderator's comments:

Mark:

Moderated

Final

Mark:

Mark:

Introduction

There are four Tasks in this assignment focusing on some very important aspects of security. The first Task is designed to offer opportunities to candidates to demonstrate their proficiency in security engineering. The second Task is about security standards, auditing and assurance procedures. The third Task is an exercise in the organisation of users and data- In the fourth Task the candidates have the opportunity to demonstrate their awareness of security vulnerabilities and their exploits.

Aims

- To develop understanding of common security issues and their corresponding solutions.
- To develop skills in analysing problems, identification of security risks, and evaluation of alternative solutions.
- To provide opportunity to students to demonstrate their hands-on skills.
- To encourage students to understand the security assurance processes and their various standards.

Task 1 – 18 Marks

Write a report of approximately 600 words covering the following: **Concepts**

a) Define the following security concepts:

- Asset
- Exposure
- Vulnerability
- Attack
- Threats
- Control

b) With reference to a Hospital Information System designed to maintain personal information on patients about their health and treatment, give examples for each one of the concepts you have defined in Task 1 a).

c) The 2nd column in the following table identifies some of the essential stages (one stage per row) of risk assessment. In order to help candidates understand, an example of each stage is given in the 3rd column of the corresponding row.

Another (2nd) example of each stage is to be filled by the candidates in the fourth column of the row.

After identifying an asset in the top row, an analyst would go through different stages and arrive at the security requirements in the bottom row. The third column shows a practical example of the assessment process from rows a-to-h.

The 4th column of the top row identifies “Hospital Information System package” as an asset in its row a) and assesses its value to the enterprise as high in row b). **You are required to fill rows c- to- h of this 4th column.**

No.	Assessment stage	First Example	2 nd example – To be filled in by the candidates
a)	Asset Identification	Individual patient record	Information system
b)	Value assessment	Low and medium	High
c)	Exposure assessment (potential losses if the asset is exposed to a threat)	Loss of reputation	
d)	Threat identification	Password compromise as users write it down	
e)	Probability assessment (of threat occurring)	Possible if audit control is not in place	
f)	Possible control to protect the asset	Audit check that passwords are kept secret and changed regularly	
g)	Assessment of cost of the control	Feasible	
h)	Definition of the security requirements	Access is denied if passwords is not changed say every fortnight	

Task 2 – 24 Marks

Security standards

Write a report of approximately 600 words covering the following:

- a) Explain the benefits of using security standards.
- b) Briefly describe the following security standards:
 - TCSEC
 - ITSEC
 - Common Standards
- c) Describe the benefits of the following types of security auditing processes, compare their distinguishing features:
 - Policy verification
 - Compliance review
 - Security review
 - Governmental review

Task 3 – 36 Marks

User Accounts, Groups, Shared folders and Encryption

This Task is designed to be performed on a machine, which has an appropriate version of Microsoft Windows installed. For each sub-Task gather evidence (screen dumps, printouts, answer questions) as proof of completing the sub-task. For the overall task your report should comprise approximately 1000 words.

- a) Log on as Administrator and create a folder “temp”. Create a document “temp.doc” in this folder. Create a new user named “John” with password “test” as a member of “Users”. Share the folder along with its files and set permissions for John to have shared access to the folder. Log on as John, find the temp, and check whether it is shared or not. If not, explain why the folder is not shared. How can you make sure that John’s shared access as intended is enforced?
- b) Perwaiz is a member of a group on a machine connected to the network. Give shared access to Perwaiz for the folder temp and the file temp.doc. Apart from share permissions you can also grant file and folder permissions. Demonstrate permission management by using the combination of the two mechanisms.
- c) Use the console to view any personal digital certificate installed on your machine. Print the certificate. Get a digital certificate which is available free or for test purposes from any certification authority and install it in your browser. Use the console to check that the certificate has been installed properly.
- d) Create two users named “Ian” and “Najam” both having the password “test”. Create a folder “Anothertemp” containing a document “Anothertemp.doc” and set shared access to them for Ian as well as for Najam. Once Najam and Ian both have shared access to Anothertemp and Anothertemp.doc, experiment with different possibilities of encryption, decryption, and other administration tasks to answer the points raised below. Making references to the results of your experimentation, document your observations and explanations about the following:
 - 1) Can Ian access files encrypted by Ian or Najam and why?
 - 2) When logged on as Ian, can Ian be made a member of other groups?
 - 3) What happens when encrypted files are moved about?
 - 4) What happens when encrypted files are copied to an unencrypted folder on the same volume?
 - 5) What happens when encrypted files are copied to a volume that is not NTFS e.g. FAT or a floppy disk?
 - 6) What happens when you try to encrypt the system files?
 - 7) What happens when you try compressing the encrypted files?

Can Ian share his encrypted files with Najam? Give technical reasons to support your reply.

Task 4 – 22 Marks

Denial of Service Attack

- a) Briefly describe the common Internet vulnerability known as Distributed Denial of Service (DoS) attack. Your description should be approximately 800 Words in length and include answers to the following:
- 1) What is a Distributed Denial of Service attack?
 - 2) How is a DoS executed against a website?
 - 3) How can you prevent your personal computer from being used as a DoS host?
 - 4) What should you do if you find a DoS host program on your computer?
- b) Download a scanning tool from <http://www.nessus.org> and scan your desktop computer to find vulnerabilities, if any, and fix them. Produce screen dumps and printouts as evidence of completing this task.

Guidance

It is vitally important that candidates use their tutors as support and as a resource throughout the assignment.

The assignment Tasks require a considerable amount of theoretical background knowledge as well as product specific knowledge. Candidates can enrich their knowledge by searching the Web and making use of any reference library before embarking upon the practical aspects of the assignment. Candidates should fully complete a Task and consult with their tutor for guidance before starting the next Task.

Submission Requirements

A single word-processed document containing all documentation i.e. explanations, output reports and page images of graphic tools etc. pertaining to the four Tasks. In particular it should include the following:

- The solutions to the four Tasks.
- All information / data that can be used to test various aspects of your work on an appropriate medium (zip disk and CD-ROM etc.).
- Output of testing and experimentation on an appropriate medium (floppy disk, zip disk and CD-ROM etc.) in a form, which can be run DIRECTLY from the supplied media.
- Screen dumps should be produced in support of your explanations where possible.
- The document should be signed and dated by your tutor.
- The document should be submitted both in paper form and digital form on a disk.

Warning: All media must be virus free!

Media containing viruses, or media which cannot be run directly, will result in a FAIL grade being awarded for this module.

**You must read and understand NCC Education's policy on 'Academic Dishonesty and Plagiarism'.
You must complete the 'Statement and Confirmation of Own Work' form and attach the completed form to
your assignment.**