Q 1 (a) Describe the Software Waterfall Lifecycle Model.

The “Waterfall Model” is an early linear model that represents a method as to how software can be developed. It was developed by Winston W. Royce in 1970 in his paper "Managing the Development of Large Software Systems". The main stages of the “Waterfall Model” are:

System Requirements: Identify, select and document functional, scheduling and financial requirements.

Software Requirements: Identify, select and document the software features necessary to satisfy the system requirements.

Analysis: Methodically work through the details of each requirement.

Program Design: Use programming techniques to design software and hardware within the constraints and objectives set in the earlier stages.

Coding: Implement the program as designed in the earlier stages.

Testing: Test the software and record the results.

Operations: Deliver, install and configure the completed software.

3(b) Explain what a *Denial-of Service Attack* is, including an example.

Makes the "victim" computer unavailable to its users. Typically used on computers that act as Web Servers. Works by making the "victim" computer perform a task over and over again, thus preventing it from doing other jobs. For example, if the computer is supposed to take orders from customers, and the first step is for the "victim" computer to identify itself to the customer computer, a DoS attack might keep making the "victim" computer identify itself and therefore unable to do other work.

For example, a HTTP POST DoS attack.A legitimate HTTP POST header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (e.g. 1 byte/110 seconds). Due to the entire message being complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, which can take a very long time. The attacker establishes hundreds or even thousands of such connections, until all resources for incoming connections on the server (the victim) are used up, hence making any further (including legitimate) connections impossible until all data has been sent.