CSC 437 Computer Security
Instructor: Dr. Natarajan Meghanathan

Question Bank for Module 6
Denial of Service Attacks

1) What is IP Spoofing? How is it related to Denial of Service attacks?

2) What is port scanning? What are its benefits? Explain its role in Denial of Service of attacks?

3) Briefly explain how would you launch each of the following attacks and any solution that you would adopt to prevent/avoid or at least mitigate them?
   a. Ping of death attack
   b. Smurf attack
   c. Echo-Chargen attack
   d. SYN Spoofing attack

4) Distinguish between local and blind session hijacking.

5) What critical details of a TCP session an attacker has to know to hijack the session?

6) What is TCP ACK storm? How is it generated during TCP session hijacking? Explain using an example the sequence of message exchanges, starting from TCP connection establishment, that would trigger a TCP ACK storm. Indicate only the values of the critical parameters that you think are needed to trigger this attack.

7) Assuming no packet filtering occurs at the routers based on the destination IP address, explain the sequence of actions and the messages exchanged when an attacker inserts a packet that has the following information in its network and transport layer headers?
Source IP address 130.10.1.1
Source port number 7
Destination IP address 150.34.255.255
Destination port number 19

8) Redo Question 6 if the destination IP address is 150.34.1.2 and the port number is still 19.

9) Briefly explain the following attacks with appropriate examples:
   a. DNS Cache Poisoning b. Teardrop attack c. Traffic Redirection

10) What is a zombie? How is it used to launch a Distributed Denial of Service Attack?

11) Explain the security attack that can be used by an attacker to trick a browser to sending a cookie or file to a rogue server?

12) Describe the three gateway router/firewall-level solutions discussed in class to combat Denial of Service attacks.

13) Describe the two Internet layer solutions discussed to prevent Denial of Service attacks.

14) Describe the two transport layer solutions discussed to prevent Denial of Service attacks.