CSS 322 – QUIZ 8

First name: _____ Last name: _____

ID: _____ Total Marks: _____

out of 10

Question 1 [1.5 marks]

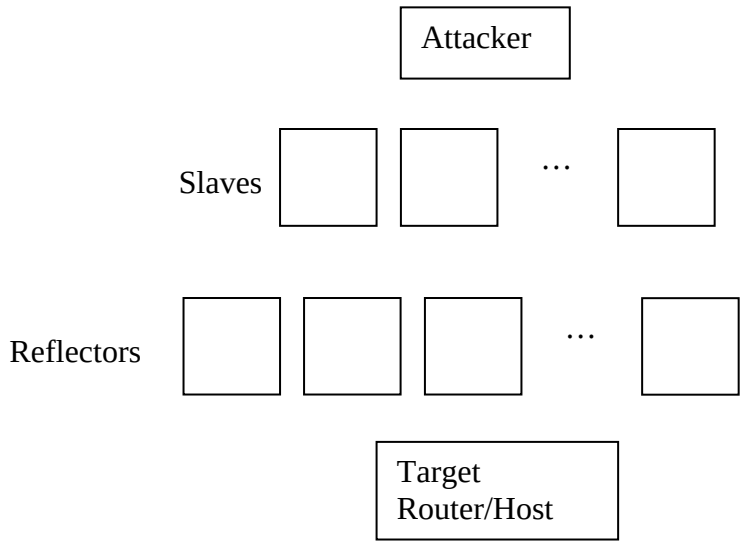
Explain why an attacker may supply a new Instruction Pointer when performing a buffer overflow attack. Make sure you mention what value the new IP should have.

Question 2 [1.5 marks]

Explain why the C function `strncpy()` should be used instead of `strcpy()` if you want to avoid (or minimise) buffer overflow attacks.

Question 3 [2.5 marks]

Explain how an ICMP (Ping) flood distributed denial of service attack works. Use the diagram below to identify the main steps taken.



Question 4 [3 marks]

Fill in the tables to create firewall rules that perform the following actions on a local network with address 203.131.209.0 (subnet mask 255.255.255.0). You can assume that by default, all traffic will be accepted. You can refer to entire networks by their network address, e.g. 203.131.209.0 refers to all computers on the local network. You can use * to many 'any'.

a) Block all traffic to any server on the local network.

Rule	Source IP	Source Port	Dest IP	Dest Port
1				

b) Block traffic from client 203.131.209.3 on the local network to web servers on the network 64.233.189.0 (with subnet mask 255.255.255.0).

Rule	Source IP	Source Port	Dest IP	Dest Port
2				