CSS 322 – QUIZ 8 ANSWERS

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.

If the attacker supplies both malicious code (to be stored in memory) and a new Instruction Pointer, then they new IP is used to overwrite the old IP so that the calling program will continue execution from when the new IP points to in memory (rather than to where the old IP points to). The new IP should point to the start position in memory of the malicious code (hence the malicious code will be executed).

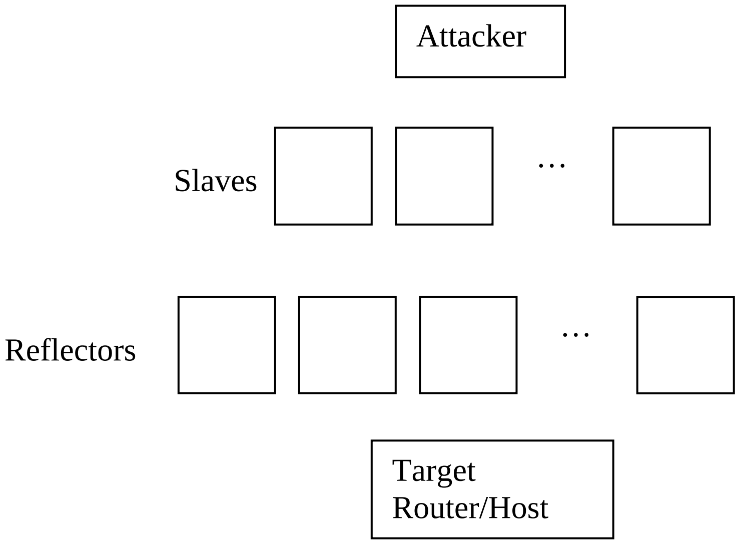
Question 2 [1.5 marks]

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

strcpy(dest,src) while strncpy(dest,src,n) where n is the number of characters to copy from the source string to the destination string. By forcing the programmer to specify the number of characters to copy, it leaves little chance of an attacker from supplying a large source string (that could contain malicious code and a new IP) that overflows the destination buffer.

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.



The attacker (we assume it has control of slaves) triggers the slaves to send a PING request to a large random set of reflector nodes. The slaves spoof (or fake) the source IP address: they set the source IP address to that of the target, instead of the slave. When the reflectors receive the PING request they send a PING response to the source of the request – that is, the target. Hence the target is overflowed with traffic as well as computing resources in handling the PING responses.

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	*	*	203.131.209.0	*

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	203.131.209.3	*	64.233.189.0	80