

## CSS 322 – QUIZ 8A

First name: \_\_\_\_\_ Last name: \_\_\_\_\_

ID: \_\_\_\_\_

Total Marks: \_\_\_\_\_

out of 10

### Question 1 [3 marks]

*Multiple choice. Select the most accurate answer. Choose only one. You receive 1 mark for a correct answer. You lose 0.5 marks for an incorrect answer. 0 marks for an unanswered question.*

1. The Diffie-Hellman exchange in Transport Layer Security (TLS/SSL) is used for exchanging:
  - a) Secret values between two users
  - b) Certificates between two users
  - c) Nonce values between two users
  - d) Sequence numbers between two users
  - e) Encrypted files between two users
  
2. Stateful packet inspection:
  - a) Allows a firewall to reject (drop) packets based on the content of emails (e.g. spam, viruses)
  - b) Allows a firewall to reject (drop) packets that contain malicious HTTP GET requests
  - c) Allows a firewall to reject (drop) packets that do not belong to an open TCP connection
  - d) Requires a dual homed bastion host
  - e) Requires a screened subnet with demilitarized zone (DMZ)
  
3. If you had access (e.g. login as an administrator) to the SIIT gateway router, for all messages passing through that router, you could:
  - a) Read the contents of the messages if they were encrypted only with TLS
  - b) Read the contents of the messages if they were encrypted only with IPsec (transport mode)
  - c) Read the contents of the messages if they were encrypted with any encryption algorithm/protocol.
  - d) Not read the contents of the messages if they were all encrypted with IPsec (transport mode)

### Question 2 [2 marks]

If ESP in transport mode is used in IPsec when sending a HTTP request, select which pieces of information are authenticated (you may select more than one – you must get all correct to receive full marks):

- a) Mutable fields (those that may change) in the IP header
- b) The headers from Physical and Data Link/MAC layers
- c) The Authentication Data field in the header
- d) The first 96-bits of the payload
- e) The TCP header
- f) The entire IP header
- g) The HTTP request

**Question 3** [2 marks]

Assume SIIT Bangkadi network is connected to SIIT Rangsit network via the public Internet. Explain an advantage and disadvantage of using IPsec in tunnelling mode (versus transport mode) to secure traffic between the two networks.

*Advantage of tunnelling mode*

*Disadvantage of tunnelling mode*

**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 mean 'any'.

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

Rule	Source IP	Source Port	Dest IP	Dest Port
1				
2				
3				

- 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
1				
2				
3				