UNIVERSITY OF NEW BRUNSWICK
Faculty of Computer Science
Network Security (CS4415-CS6415) – Winter 2021
Midterm – 30 minutes
(+ 2 minutes for uploading the answer sheet.)

1. List and briefly define categories of passive and active security attacks. Active attacks are the ones which actually leave a trace of themselves and modify something such as man in the middle attack, ddos/dos. or even routing attacks in iot where they drop some of the packets . passive attacks just focus on gaining information and stealing data, such as traffic sniffing.

2. List and briefly define categories of security services. Authentication:it verifies whether the both sides of the communication are the ones the claim to be, confidentiality: it does not allow the sensitive information to be leaked and accessed by intruders (it uses encryption) , integrity: it ensures the transferred packets are not modified , non repudation : it ensures that the sender can not deny their actions. Availability: it ensures the service resources are only used by legitimate users

3. List and briefly define the SSL/TLS protocols. Record protocol , handshake protocol: the two sides exchange the certificates and keys and encryption algorithms before transferring data, changeCypher: it exchanges the encryption and security algorithms, heartbeart: it makes sure the other side of the communication is alive , alert : it is used to notify the sender and receivers about failure in transferring data.

4. List and briefly define the SSH protocols. Transport protocol : used for server authentication, communication protocol: it creates multiple channels within the communication , user authentication: it authenticates the client

5. What is Base-64 conversion and why is it useful for an E-mail application? It is a compatibility scheme used in MIME

6. Among the listed network security solutions in 3 layers, which one is the most robust solution and why (Two reasons)? s/mime because It covers all fundamental security aspects (by using encryption , digital signature and also optionally compression)and moreover it offers enhanced security features such as security labeling

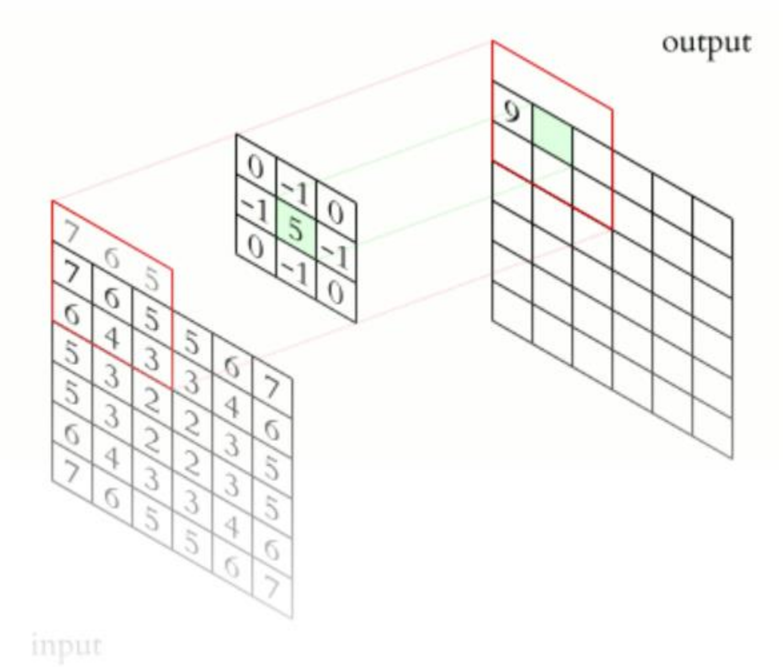
7. List and briefly explain the five steps of the TLS record protocol operation. It fragments the data and then compress them and then it adds the MAC and finally it encrypts the whole record and then appends the header.

8. Briefly explain two different modes of IPSec. Tunnel mode : it encrypts the whole packet and the original ip address. Transport mode : it does not encrypt the original ip but encrypts the rest of the packet

9. Briefly explain two mail access protocols. IMAP and POP3 , IMAP can handle multiple clients working with it, and it always leaves the emails on the email server whereas POP3 lets us download the emails on our machine and deletes it from the server.

10. List and briefly explain four virus phases. Dormant phase: this is the phase where virus is waiting and does not do anything , propagation phase : this is the time when virus replicates itself, Triggering phase: this is the phase when the corresponding event is fired and virus must act. and executing phase : this is the phase when the virus actually executes the malicious payload

11.


output
9
7 6 5
7 6 5 5 6 7
6 4 3 3 4 6
5 3 2 2 3 5
5 3 2 2 3 5
6 4 3 3 4 6
7 6 5 5 6 7
0 -1 0
-1 5 -1
0 -1 0
input
