

CS 409 **Ethical Hacking**

Homework 2

(30 pts)

1. What are the communication identifiers that are used in the Data link layer, Network layer and Transport layer? How does Internet Assigned Numbers Authority (IANA) maintain a list of port number assignment?
2. What is an IP address? Describe the general structure of IP address. How does the IP address divide during subnetting?
3. Describe the TCP connection establishment, termination and reset mechanisms.
4. Describe the major differences between TCP and UDP. Mention four disadvantages of UDP port scanning.
5. Explain the stages of a hacking cyber-operation in your own language.
6. What is port scanning? Mention different types of port scanning techniques with their advantages and disadvantages.