IE2022 - Introduction to Cyber Security
Year 2 Semester 1
Tutorial 01

1. Define Computer Security and Information Security.

2. Explain what integrity, availability and confidentiality is with respect to information security.

3. What is the difference between passive and active attacks in networks? Give one example per each.

4. What is the difference between inside attacks and outside attacks? Give one example per each.

5. What are the benefits gained by implementing proper accountability in computer systems?

6. RFC 2828 document defines four kinds of threats: unauthorized disclosure, deception, disruption, and usurpation. List two example attacks for each.

7. Define Security Assurance.

8. A security strategy should include three aspects including correctness/assurance to see if the strategy works. List two ways to ensure correctness/assurance.

9. Briefly explain the following terms.

    i). Vulnerability
    ii). Exploit
    iii). Threat
    iv). Attack
    v). Adversary
    vi). Risk
    vii). Countermeasure

10. Evaluate the importance of vulnerability assessments and penetration testing for modern-day organizations managing IT infrastructure.