Seminar 7 (Week 7)

Q1. Please perform the following activities in group:

I. Please read the A Taxonomy and Terminology of Adversarial Machine Learning from this link (https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8269-draft.pdf)
II. Please focus on the attacks and try to understand the attacks by discussing them with peers and Lecturer/tutors.
III. Please think about the defense mechanisms and their limitations.
IV. Please think about Generative AI, how they can be attacked. Discuss with peers and Lecturers/tutors. Please feel free to Google.