CS5260 Project Proposal - GAN for Product Recommendation System

* (Product) Recommendation System (https://www.datacamp.com/community/tutorials/recommender-systems-python)
  + Collaborative Filter (clustering, time series…)
    - Similar users - clustering
    - Previous behavior - MDP
  + Content Filter (product & user characteristic)
    - Product image (CNN)
    - Comments (NLP – attention, bert...)
    - Other meta-data (e.g. genre, age, description, category…)
* Adversarial Attack to (Product) Recommendation System
  + Attack to (MLP/decision tree) meta-data (logits/numerical features) (GAN -> MLP/decision tree)
  + Attack to (CNN) image data (GAN -> CNN)
  + Attack to (NLP) comments (GAN -> Bert: text generator)
* Training (Product) Recommendation System using Adversarial samples – GAN

Ref:

1. https://arxiv.org/pdf/2007.07269.pdf
2. <https://arxiv.org/pdf/2005.10322.pdf>
3. <https://iopscience.iop.org/article/10.1088/1742-6596/1405/1/012005/pdf>
4. <https://arxiv.org/pdf/1809.07062.pdf>
5. <http://sundaram.cs.illinois.edu/pubs/2018/2018kirshnan_ncf.pdf>

api

* <https://adversarial-robustness-toolbox.readthedocs.io/en/latest/>
* <https://towardsdatascience.com/evaluating-adversarial-examples-with-similarity-metrics-in-python-13acb9b5fa9f>
* <https://realpython.com/generative-adversarial-networks/>