Department of CSE, IIT (BHU)

Undergraduate Project Plan

Title: Network Intrusion Detection in an Adversarial Setting

Team: Name - Shreyansh Singh Roll No - 16075052

Supervisor(s): Prof. K.K. Shukla

Objective:
To break classifiers trained for Network Intrusion Detection by supplying them with Adversarial examples.

Deliverables / Achievables:
To learn about ML and DL being used for Network Intrusion Detection Systems (NIDS). Learning about various attack techniques for genearting adversarial examples.

Work Plan:
I. Week-wise/ Month-wise plan for Semester VI

1st Month – Literature survey on applying ML to the NSL-KDD dataset, a dataset used for training models for NIDS
2nd Month – Learning about different Adversarial attack techniques
3rd Month – Implementing ML and DL models for NIDS
4th Month – Applying adversarial attacks and generating adversarial examples

II. Broad overview plan for Semester VII
Techniques for making the models more robust aginst Adversarial examples.

I plan to work according to the above plan.

Signature of students with name,:

1.

The above plan is approved.

Signature of Supervisor(s) with date ___________________________________