Computer Network Project CNT 4713

Data Analytics for Inferring Probing Activities

You are given a **darknet dataset** (http://public.eng.fau.edu/ebouharb/14.7z) representing one day of unsolicited Internet traffic. (To understand what is darknet data, please refer to https://www.researchgate.net/profile/Claude_Fachkha/publication/283827224_Darknet_as_a_Source_of_Cyber_Intelligence_Survey_Taxonomy_and_Characterization/links/5656265a08ae1ef92979db33.pdf) The aim of the project is to build a cyber-security capability that permits the **inference** (i.e., detection) of **probing activities** by analyzing the darknet IP space.

A complete project necessitates the development of a simplistic **back-end** and an **API**.

The back-end (1) aims at analyzing the dataset to infer **sources of IP addresses** which are related to **probing activities**. The back-end should also (2) infer the **type of the probing** (horizontal, vertical or strobe), the **rate** (packets/sec) of the events, and their **start and end times**. The API should allow **querying** of the extracted information (possibly indexed in a database) to extract those IP addresses and their information (for sharing such cyber threat intelligence).

Notes:

- The projects will be assessed (i.e., graded) based on the **completeness** of their components and the **architectural/design choices** of the implementations.
- The projects can be developed using **any language/technology**.
- The projects are to be completed **individually**.

Due Date:

The project should be presented by
December 12th, 2018 at 6 pm

Good Luck