Software Project Management Plan

Project Name: Network Traffic Analyzer for Detecting Dos Attack Using Machine Learning

Customer: - Center for Development of Advanced Computing.

Project Guided by: - Mr. Muraleedharan N

Start Date: - 2nd December 2019

End Date: - 28th January 2020

Abstract:-

At any given time the traffic entering the network may be genuine or can be some malicious traffic. There may be times when a definite pattern is established when the malicious traffic is highly active(based on timelines).It becomes necessary to analyze all the incoming traffic into a particular network server to identify the types of traffic entering so that proactive measures can be taken to safeguard our systems against harmful traffic. To safeguard our System from Denial of service attack, we are implementing a system named "Network Traffic Analyser for Detecting Dos Attack Using Machine Learning".

Introduction:-

The Software Project Management plan (SPMP) for "Network Traffic Analyser for Detecting Dos Attack Using Machine Learning"analysis the incoming packets and determines whether it is normal traffic or some malicious packets in particular denial of service attack. Using machine learning the system is trained to classify the incoming traffic as normal traffic or Dos attack. The tools used to achieve this are Tshark, anaconda navigator, Matplotlib and Scikit learn. Using Tshark the incoming packets are captured and sent as a CSV file to Pandas which perform data analysis to differentiate normal packets and Dos packets and then we visualize (Bar graphs) the normal and Dos packets by using Matplotlib later, we implement ML to train the System so that it will detect and classifies the Dos packets.

Scope and complexity estimate

Here, the Scope is to analyze the network traffic, detect the Dos packets and prevent the internal network from Dos attack.

- Maintaining the traffic data.
- Handling Maximum traffic at any Point.
- Capturing the Dos attack.

Project time estimate

The amount of time to complete the project is 8-9 weeks

Resources estimate:

Project Mentor.

Mid – Review.

Final – Review.

There will be approximately 5 resources required to complete the project in given tenure which includes 1 resource to generate the traffic,1 resource for capturing the traffic, 1 resource for analyzing the traffic, 1 resource for detecting Dos attack and 1 resource to stop the attack.

Milestone schedule

This is the heart of the Project Plan. Here we list everything and everyone needed to deliver the project and we set specific dates for each task to be completed. An example milestone schedule:-

S.NO	Milestone	Responsibility	Start Date	End Date
1	Planning	All Team members	02/12/2019	03/12/2019
2	Allocation of Responsibilities	Team Lead	6/12/2019	7/12/2019
3	Learning About Tshark	All Team members	8/12/2019	9/12/2019
4	Learning About Pandas/ NumPy	All Team members	10/12/2019	17/12/2019
5	Learning About Matplotlb	All Team members	18/12/2019	19/12/2019
6	Learning About Scikit Learn	All Team members	20/12/2019	26/12/2019
7	Documenting the Findings	All Team members	27/12/2019	30/12/2019
8	Software Installing and Configuration	All Team members	01/01/2020	02/01/2020
9	Implementation	All Team members	03/01/2020	22/01/2020
10	Testing the Findings	All Team members	23/01/2020	24/01/2020
11	Make Improvements	All Team members	25/01/2020	26/01/2020
12	Mid Review	Faculty	02/01/2020	02/01/2020
13	Final Review	Faculty	28/01/2020	28/01/2020
14	Making Final Improvements	All Team members	27/01/2020	29/01/2020
15	Final Report	All Team members	30/01/2020	30/01/2020

Roles and responsibilities:

Once the resources have been identified,specific responsibilities are listed for the project team members.The listed members of our project are:-

1) Anshul, 2) Akhil, 3) Bhargavi, 4) Sumesh and 5) Chandan.

We have distributed the roles among ourselves which includes the following

Names	Roles
Anshul	Case study and Subject matter Documentation
Akhil	Exploring tools regarding implementation
Bhargavi	Case study and Subject matter Documentation
Sumesh	Analyzing tools and report
Chandan	Configuration and setup