DDOS ATTACK USING MACHINE LEARNING TECHNIQUES

DOMAIN:MACHINE LEARNING AND NETWORK SECURITY

Mentor:Arun N(H.O.D)

NAME: Utpal Balse
BRANCH:Information Science *and Engineering* USN:18BTRIS051

NAME: Purvasha Padhy
BRANCH: Information *Science and Engineering* USN:18BTRIS031

NAME: Rakesh C S
BRANCH: Information Science *and Engineering* USN:18BTRIS033

Abstract *- The definition of a Distributed Denial Of Service(DDoS) are requests sent to many computer systems or servers computer systems or servers over multiple targets, causing a flood of incoming requests which corrupts the system, causing it to shut down or become inactive. DDoS challenges the CIA triad(Confidentiality, Integrity, Availability).*

We want to create a system which uses a machine learning based implementation to detect and classify common types of network traffic flows. We will be examining multiple different sources of datasets which have a mixture of various modern types of attacks. We will be using machine learning tools to train the model to classify DDoS attacks and apply algorithms to produce our desired results. In this project , we put up with a DDoS attack detection system on the source of the operating system, based on machine learning techniques. This system comes up with statistical data from the Operating system environment to the virtual machines, to prevent different network routes from withdrawing out from the network. We evaluate diverse machine learning algorithms and carefully compare their performance.

INTRODUCTION

DoS and DDoS assaults are currently a big danger to the Internet. This threat, in the form of Internet availability, is a major issue that is impeding the growth of online businesses, which rely on their websites being accessible to users.In this paper we analyze some of the major Dos/DDos attacks using the traffic analyser, wireshark and discuss the efficient machine learning algorithms to find the patterns. We use these patterns to identify if certain network traffic is a DDoS attack or not. The definition of a Distributed Denial Of Service(DDoS) attack is where many attacks are targeted by a malicious hacker who intends to compromise systems by sending multiple requests to the server causing a server to be entirely unresponsive or shutdown.

A Denial of Service (DoS) assault, on the other hand, often entails a significantly lower volume of traffic, coming from a single source one device DDoS puts the CIA (Confidentiality, Integrity, and Availability) triad to the test.We want to create a system which uses a machine learning based approach on determining and to find out what type of an attack has occurred to a particular system. We will be examining multiple different sources of datasets which have a mixture of various modern types of attacks. We will be using machine learning tools to train the model to classify DDoS attacks and apply algorithms to produce our desired results.

Methodology

Our research is mainly composed of DDoS detection using machine learning by implementation of ANN(Artificial Neural Network). Problem: Context of the problem is finding multiple methods in order to reduce large amounts of multi data and to determine common attacks. Solution: literature survey provided us with many machine learning techniques in order to Dimensionally reduce data. Most promising results were registered by an algorithm called ANN. The expansion of ANN is Artificial Neural Networks which will include systematic steps in order to train, test and find data accuracy