Detection and Prevention of Advanced Persistent Threat (APT) activities in heterogeneous networks using SIEM and Deep Learning

Abhinaya PB
Department of Computer Science Engineering
Amrita School of Engineering
Amrita Vishwa Vidhyapeetam
Coimbatore- India

cb.en.u4cse17301@cb.students.amrita.edu

Aradhana J
Department of Computer Science Engineering
Amrita School of Engineering
Amrita Vishwa Vidhyapeetam
Coimbatore- India

cb.en.u4cse17308@cb.students.amrita.edu

In Affiliation with,

T.Senthil Kumar
Associate Professor
Computer Science and Engineering Department
Amrita Vishwa Vidyapeetham

senthilkumar@cb.amrita.edu

Sulakshan Vajipayajula,
Architect-CTO Office
IBM

svajipay@in.ibm.com

Code Developed as part of IBM Funded Project :

Detection and Prevention of Advanced Persistent Threat (APT) activities in heterogeneous networks using SIEM and Deep Learning

The organization consists of different networks at various geographical locations. For such vast networks a simple honeypot is not enough to decoy attackers. Hence, a collection of various honeypots installed at various geographically separated locations inside the organization is necessary for luring attackers. Such a conglomeration of honeypots – *Honeynet* – is the key in collection of attacker data and traffic destined at the organization. Heterogeneous data from Network devices, Systems, Firewalls, NIDS, UTMs, etc., are collected at a centralized location using *Cloud basedSplunk Security Information and Event Management (SIEM)* for further processing. Extracting useful information from a plethora of heterogeneous data is a difficult task. SIEM is supported with a *Correlation Engine* for processing such heterogeneous data. The Correlation Engine is capable of deploying Complex Event Analysis techniques, Data Mining techniques, Deep Learning algorithms, Log Analysis techniques, etc., for searching the presence of attack vectors (or anomalous behaviour). The output of the Correlation Engine can be categorised to rank the output network behaviour in terms of the severity of the data/traffic by using a metric such as *Vulnerability Score*. The dashboard of the SIEM machine is capable of displaying the near real time processing of the various network and host events, network traffic flow statistics, system behaviour, and other properties of the network.

OurTeam Specific contribution:

With the emergence of technology everyday, the devices around us are becoming smarter as a wide range of appliances are getting connected to the internet. These devices are also the least protected and thus more vulnerable to cyber attacks.This has already come true when the Mirai botnet, composed mainly of embedded and IOT devices attacked several targets with the Distributed denial of service(DDoS) attacks. Intrusion Detection Systems(IDS) play a major role in detecting possible security breaches in a network. Various machine learning algorithms have been proven effective inorder to detect such breaches. Distributed denial of service(DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server. Therefore, in this paper, more focus and understanding is laid on a few Deep Neural Network(DNN) approaches such as Multi-Layer Perceptron(MLP), Convolution Neural Network (CNN), and Recurrent Neural

Network(RNN) to detect and classify DDoS attacks specifically. The above mentioned algorithms along with a few machine learning algorithms are compared based on the following performance metrics such as accuracy, precision, F1-score, True Positive Rate, False Positive Rate and Receiver Operating Characteristics (ROC) curve to check for effectiveness.

Keywords: Deep learning, Deep Neural Network, IoT botnet, Intrusion Detection Systems, Distributed denial of service, Machine learning