Application of Machine Learning with Traffic Monitoring to Intrusion Detection in Kubernetes Deployments

Irene Ann Tony, Masters in Computer Science
University of Dublin, Trinity College, 2021

Supervisor: Dr. Stefan Weber

Kubernetes has many methods to detect an attacker attempting to attack a Cluster such as firewalls and an Ingress API. However, it does not have any built-in solutions to detect whether an attacker is already inside. There are existing solutions involving the identification of malicious traffic and they have inspired certain aspects of the solution proposed in this dissertation.

This dissertation focuses on the ways to detect malicious activity inside the Kubernetes Cluster by monitoring the internal network traffic and detecting suspicious traffic with the help of machine learning. This research focuses on TCP and UDP packets between Pods and examines them to determine whether they are malicious or not. The proposed solution involves capturing all the traffic within the Node including the communications between Pods. The solution model sits inside a Node within a Pod and is implemented by passing the captured internal traffic through a neural network that is trained to detect different characteristics of malicious packets and flag the packets that seem suspicious.

This research provides a foundation for advanced studies in detecting malicious activity within a Kubernetes Cluster using traffic monitoring and machine learning. The proposed solution can be extended to learn to detect many different types of malicious activity.