Detection of Denial of Service attack in cloud based Kubernetes using eBPF

ABSTRACT

Kubernetes is an orchestration tool that runs and manages container-based workloads. It works as a collection of different virtual or physical servers that support multiple storage capacities, provide network functionalities, and keep all containerized applications active in a desired state. It also provides an increasing fleet of different facilities, known as microservices. However, Kubernetes' scalability has led to a complex network structure with an increased attack vector. Attackers can launch a Denial of service (DoS) attack against servers/machines in Kubernetes by producing fake traffic load, for instance. DoS or Distributed Denial of service (DDoS) attacks are malicious attempts to disrupt a targeted service by flooding the target's service with network packets. Constant observation of the network traffic is extremely important for the early detection of such attacks. Extended Berkeley Packet Filter (eBPF) and eXpress Datapath (XDP) are advanced technologies in the Linux kernel that perform high-speed packet processing. In the case of Kubernetes, eBPF and XDP can be used to protect against DDoS attacks by enabling fast and efficient network security policies. For example, XDP can be used to filter out traffic that is not authorized to access the Kubernetes cluster, while eBPF can be used to monitor network traffic for signs of DDoS attacks, such as excessive traffic from a single source. In this research, we utilize eBPF and XDP to build a detection and observation mechanism to filter out malicious content and mitigate a Denial of Service attack on Kubernetes