ENHANCING INTRUSION DETECTION SYSTEM USING XDP with eBPF

ABSTRACT

Intrusion Detection Systems (IDS) play critical role in safeguarding network infrastructure from unauthorized access and malicious activities. The integration of XDP (eXpress Data Path) technology with eBPF (extended Berkeley Packet Filter) enhances the performance and capabilities of an IDS in detecting DOS(Denial of Service), DDOS(Distributed Denial of Service) attacks at Kernal space. eBPF enables custom code execution within the Linux kernel, while XDP provides a high-performance data path for packet processing. XDP programs are written in eBPF bytecode, and are attached to network devices. By intercepting incoming network packets at the NIC, XDP enables rapid processing before reaching the kernel network stack and act on the packet directly on the NIC. This combined XDP and eBPF approach represents a potent advancement in network security, providing a robust toolset for defending against a wide range of modern cyber threats, including DoS and DDoS attacks. By leveraging these technologies, we aim to achieve faster and more efficient packet analysis, enabling the IDS to respond to threats in real time.

Team Members

K Geethika Reddy – 20WH1A1270

G Krishna Prathibha – 20WH1A12B0

G Sneha – 20WH1A12B5

Internal Guide

Name: Mr. N. Anand

Designation: Assistant Processor