BVRIT HYDERABAD
College of Engineering for Women
Department of Information Technology

Mini Project - Academic Year 2023-24

TEAM 7

Enhancing Intrusion Detection System using XDP with eBPF

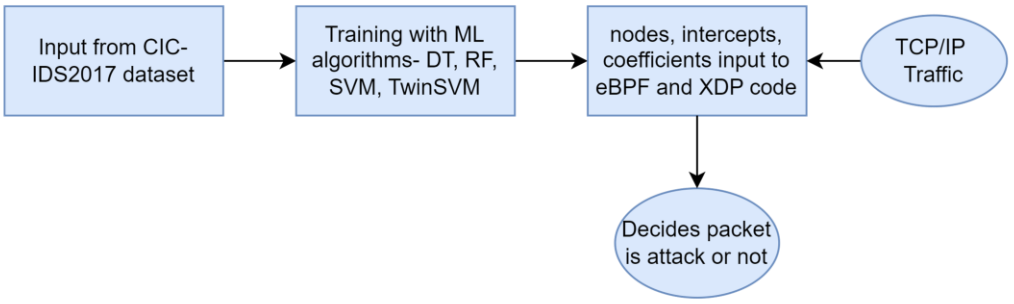
Abstract

Intrusion Detection Systems (IDS) are vital for network security, and integrating XDP (eXpress Data Path) with eBPF (extended Berkeley Packet Filter) enhances IDS capabilities in detecting DOS and DDOS attacks at the Kernel space. XDP intercepts packets at the NIC for rapid processing, leveraging eBPF's custom code execution within the Linux kernel. This dynamic duo allows for high-performance packet analysis directly on the NIC, strengthening the IDS against unauthorized access and malicious activities. The approach represents a significant advancement in network security, providing a potent toolset for real-time threat response, particularly against DoS and DDoS attacks.

Modules

- **Feature Extraction from dataset**
- **Training ML algorithms – DT, RF, SVM, Twin SVM**
- **eBPF wrapper**
- **Adding to XDP**

Architecture



Tools and Technologies

- **ML algorithms – Decision Tree, Random Forest, SVM, Twin SVM**
- **eBPF and XDP**

Conclusion and Future Scope

The performance of the Intrusion Detection System has been increased using XDP and eBPF together, the results shows that the packet processing per seconds has been increased to about 50% in kernel space than in the user space. The future scope of this work extends to exploring the integration of various machine learning algorithms with XDP and eBPF to elevate the performance and accuracy of Intrusion Detection System.

Guide Name

Mr. N. Anand

Assistant Professor
anand.n@bvrithyderabad.edu.in

Team Members

K. Geethika
20WH1A1270

G. Krishna Prathibha
20WH1A12B0

G. Sneha
20WH1A12B5

Github links

1. https://github.com/geethikareddyk9/Enhanced-IDS
2. https://github.com/prathibha101/Mini-project
3. https://github.com/Sneha-Gunjari/Mini_Project2k23