Network Security Project-Implemented features

Masoud Erfani

December 6, 2019

To detect the DDOS attack, I have implemented two features. These features are flow duration and number of packets in a forward direction.
Flow duration is a session of packets between a source IP and port to a destination IP and port. Also, the forward direction is when the packet moves from say A to B. These features were implemented by Lopez (2019) and they are considered as two important features for detection.

According to Sharafaldin et al. (2019), Flow Duration is a proper feature for detecting SYN attack. Also, the number of forwarding packets is one of the most important features for detecting DrDoS-MSSQL attack in which, attacker abuses the Microsoft SQL Server Resolution Protocol (MC-SQLR) and sends millions of packets to the victim.

DDoS attacks have clear behavior in sending packets to the victim. This behavior affects the arrival rate and so, it affects the mention features. So, they can be used for DDOS detection.

References

Lopez, Alma D.; Mohan, A. P. a. N. 2019. Analytics for detection of ddos attacks. *SMU Data Science Review: Vol. 2 : No. 1 , Article 14.*

Sharafaldin, I., Lashkari, A. H., Hakak, S., and Ghorbani, A. A. 2019. Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)*, pages 1–8.