Mitigating a Slow DDoS attack in a software defined network

(CSC 7078) Damien McGloin 40000631

Objective

To detect and prevent a low and slow attack with a secondary goal of intrusion detection. The reasoning for this secondary goal being that malicious users often combine attacks.

Tools used to implement the project

This project will implement SDN cockpit which features a built-in traffic generator. By converting a pcap file into a trafgen configuration file via netsniff-ng it will be possible to recreate an attack in a safe environment. The mininet virtual network emulator will be used within SDN cockpit to configure a network topology. A ryu openflow controller (v1.3) will be used to implement the solution for monitoring and preventing the attack. The secondary objective of intrusion detection can be accomplished with an open-source IDS tool such as snort which will be integrated with the ryu controller. A final tool which will be employed is wireshark which offers advanced network monitoring.

Requirements

First, the creation of an application which can correctly identify a low and slow attack. A key concern is differentiating between users with a slow internet connection and users with malicious intent. This can be done by monitoring for numerous TCP handshakes followed by TCP segmented packets only, users resending incomplete HTTP headers or the absence of FIN packets [1]. Additionally, by measuring the packet rate and uniformity of the packet distances [2]. A simple network topology can be employed with a switch and three hosts representing a web server, normal traffic and the attacker. This is based on the topology outlined in a previous study [3]. An additional host will also be added to run snort to monitor for a second malicious attack such as a hydra brute force attack [4]. The measures used to deal with this attack will include rate limiting, event filtering and packet dropping [5].

Evaluation

The primary tool for evaluating the application will be wireshark as it provides a means of assessing elements such as the round-trip time of data packets being sent across the network. This will be useful in assessing the impact of the application on normal traffic as well as its ability to block malicious traffic on the network. The RTT graph tool within wireshark will be helpful for visually demonstrating this impact. Additionally, assessing data such as the packet count, byte count and error count will be essential for understanding and evaluating the application proposed here.

[1] Mazebolt, "Slowloris Attack" [Online]. Available: https://kb.mazebolt.com/knowledgebase/slowloris-attack/ [Accessed June 29, 2021]

[2] T. Lukaseder, L. Maile, B. Erb and F. Kargl, "SDN-Assisted Network-Based Mitigation of Slow DDoS Attacks" 2018. Available: Cornell University, https://www.cornell.edu/. [Accessed: June 28, 2021]

[3] T. Lukaseder, S. Ghosh and F. Kargl, "Mitigation of Flooding and Slow DDoS Attacks in a Software-Defined Network" 2018. Available: Research Gate, https://www.researchgate.net. [Accessed: June 28, 2021]

[4] X. Xu, J. Dai and Y. Zhi, "An Intrusion Prevention Scheme for Malicious Network Traffic Based on SDN" 2020. Available: IOP science, https://iopscience.iop.org/. [Accessed: June 27, 2021]

[5] R. kloti, V. Kotronis and P. Smith, "OpenFlow: A Security Analysis" 2013. Available: IEEE, https://ieeexplore.ieee.org/Xplore/home.jsp. [Accessed: June 27, 2021]