"*Undertake a project to demonstrate the application of cyber security in a softwarized network scenario*".

Objective:

The objective of this project is to successfully detect and mitigate a DDoS - SYN flood attack within a Software Defined Network environment. A SYN flood attack is a common DDoS attack that exploits the three-way handshake process of TCP connection [1]. An attacker will overwhelm the target machine with a flood of spoofed SYN packets with the goal of exhausting memory within the network by maintaining half opened connections [2], degrading the performance of the SDN controller and preventing legitimate traffic as a result. As the attacker sends the SYN request from a spoofed IP address, the SYN ACK is never received, and therefore the final ACK is never sent to the target, causing the half opened connections within the network. SYN flooding attacks can overflow the storage space or flow table in OpenFlow switches within the SDN's data plane. In addition to damaging the controller, a SYN flood attack can also break the link between the control plane and data plane. Even if the flooding attack is launched in a few seconds, the entire network can be breached or brought to a halt[2].

Tools:

SDN Cockpit, which builds on the *mininet* emulator and the *Ryu* controller, is the baseline tool for the project. -*Mininet* is a network emulator that enables the creation of virtual hosts, switches and controllers, i.e. the network topology. - *Ryu* is an SDN controller, which is located in the control plane, and communicates with the data plane via the southbound API. - *OpenFlow* is the southbound API to be used, allowing entries to be added or removed to the flow tables of the network switch. - *Hping3* will be used to generate SYN flood traffic. - *Wireshark* will monitor TCP packets. - *iperf* will measure network performance. - *Xterms* will enable interaction with interfaces for each individual host on the network. –*Python* is the programming language used to create application solution.

Design Requirements:

The SDN will consist of 4 hosts and 1 switch. Host 1 will send malicious SYN flood packets to Host 2 (fig.1), while Host 3 will send regular TCP packets to Host 4 (fig.2). The OpenFlow switch will perform packet lookup and forwarding according to flow rules in the flow table, communicating with the controller via the OpenFlow protocol.

Figure 1: SYN flood traffic from spoofed IP address

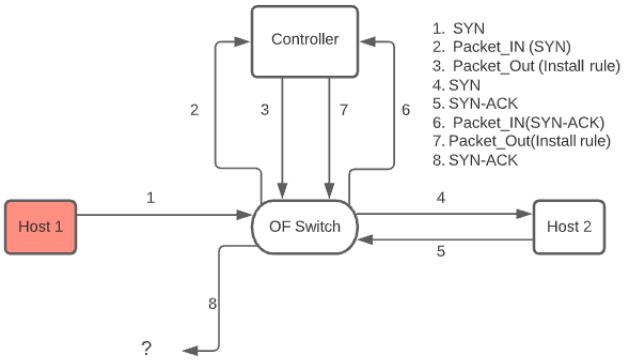
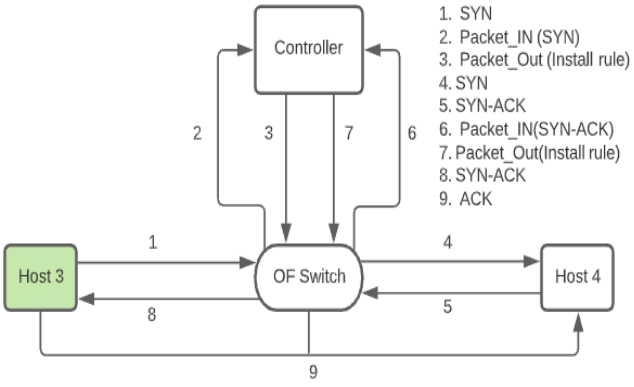


Figure 2: Legitimate TCP traffic



The proposed network topology allows for the flow of malicious SYN flood traffic, and normal TCP traffic on the network. The application, which runs at the controller, is required to monitor and count TCP SYN packets, protecting the network against a SYN flood attack, through blocking these packets when they reach a specific threshold. The network solution also must be able to differentiate between malicious traffic and legitimate TCP packets, enabling regular traffic to flow as normal, unaffected by measures in place. While the application is running at the controller, it is also important that network performance is not negatively affected by increased bandwidth.

Evaluation:

In order to test that the solution meets requirements, SYN flood traffic will be generated using Hping3, flooding Host 2 with SYN packets from Host 1, while Host 3 sends regular TCP packets to Host 4 in the background. The success of the solution will be determined by:

- Efficient detection and mitigation of the SYN flood attack, based on the packet count threshold that is set in the application, dropping packets when threshold is exceeded, and blocking future traffic from malicious source.
- Effectively distinguishing between SYN flood traffic and benign TCP packets, allowing legitimate traffic to pass through the network while application is running.
- Limited impact on network performance caused by the application running at the controller. Traffic monitoring using 'iperf' will be used to determine if latency is introduced, comparing network traffic bandwidth when application is, and is not running.

1. Cloudflare "SYN flood attack" Available: https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/ [June 28,2021].
2. Conti, Mauro, Ankit Gangwal, and Manoj Singh Gaur. "A comprehensive and effective mechanism for DDoS detection in SDN." Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2017, pp. 1-8