1. **Defender perspective.**

Due to the nature of this type of attack is to flood the targeted infrastructure with traffic or requests, the blue team’s role is to recognize signs of an attack through many symptoms suggesting that the system is being attacked including slow network performance, unavailable or inaccessible websites or sudden increase in traffics [6]. During the attacks, the defender team should identify and flag any abnormal traffic and its sources, configure the firewall and traffic rules, monitor the networking traffic [6]. The attacks could also be prevented by continuously monitoring, analyzing, and logging networking traffic information in order to distinguish a possible DoS attack, establishing a baseline between normal and abnormal network activities and working with the ISP, implementing and configuring defense perimeter, anti-DoS intrusion system[6]. Many network monitoring and DoS defending tools including Wireshark, snort, Fail2Ban, and Netfilter.