Software Defined Networks (SDN) were created to address the scalability and high maintenance costs of conventional networks. SDN is susceptible to Distributed Denial of Service (DDOS) attacks because of its scalability, programmability, and centralized control. DDOS aims to deplete the target host's resources and block authorized users from accessing it. DDOS attack detection in SDN has been accomplished using Support Vector Machine. A supervised machine learning technique called SVM searches for the hyperplane that best divides two classes. SVM features a number of kernel functions and regularization parameters that, if not properly chosen, can have an impact on performance. This study looks at some of the regularization and SVM Kernel functions that are already available, and how they function with various parameter values. The outcome demonstrates that various criteria produced diverse outcomes. The performance of the polynomial and Gaussian kernels was superior, but their computational cost was higher