Abstract

Distributed Denial of Service attack (DDoS) is a crucial issue to those in the security field. It is based on sending many malicious packets to the targeting service, causing failure of normal network services. There are a lot of defense systems developed to overcome this kind of attack. Indeed, predicting the attack at the first stages is an effective solution to give the defender certain amount of time to act. In this paper, a predictive model (Naïve Bayesian) is applied on a KSL-KDD dataset that contains six types of DDoS attack (Neptune, back, land, pod, smurf and teardrop). The model shows high accuracy of 99.99%.

References


Index Terms

Computer Science  Security

Keywords

DDoS, detection, prediction, attack.