
Abstract

In this paper we present a novel intrusion detection system which makes use of behavior profiles to identify HyperText Transfer Protocol (HTTP) tunneling activities. Behavior profiles correspond to inherent attributes of application network sessions. Our system evaluates network behaviors at two different levels: a local multi-packet level and a session level. When suspicious behavior is detected, a verification module performs a detailed analysis of the corresponding session data. Currently, our system detects both malicious and unauthorized HTTP tunneling activities. Our experimental results show the effectiveness of our system and demonstrate the validity of using packet features for anomaly detection.