A comparative study of alert correlations for intrusion detection

Abstract

The prevalent use of computer applications and communication technologies has rising the numbers of network intrusion attempts. These malicious attempts including hacking, botnets and works are pushing organization networks to a risky atmosphere where the intruder tries to compromise the confidentiality, integrity and availability of resources. In order to detect these malicious activities, Intrusion Detection Systems (IDSs) have been widely deployed in corporate networks. IDSs play an important role in monitoring traffic behaviors in a computer network, identifying the anomalous activity and notifying the security analyst with current network status. Unfortunately, one of the IDSs' drawbacks is they produce a large number of false positives and non-relevant positives alerts that could overwhelm the security analyst. Therefore, the process of analyzing alerts in order to provide a more synthetic and high-level view of the attempted intrusions is needed. This process is called Alert Correlation. In this paper, we present commonly used alert correlation approaches and highlight their advantages and disadvantages from various perspectives. Subsequently, we summarize some current alert correlation models with their alert correlation approach.