Abstract

World Wide Web is widely accessed by people for accessing services, social networking and so on. All these activities of users are traced in different types of log files. Hence, log files prove to be extremely useful in understanding user behavior, improving server performance, improving cache replacement policy, intrusion detection, etc. In this paper, we focus on the intrusion detection application of log files. By analyzing drawbacks and advantages of existing intrusion detection techniques, the paper proposes an intrusion detection system that attempts to minimize drawbacks of existing intrusion detection techniques, viz. false alarm rate and inability to detect unknown attacks. To accomplish this, association rule learning, reinforcement learning and log correlation techniques have been used collaboratively.

References

Index Terms

Computer Science    Network Security

Keywords

Association Rule Learning  Log Correlation  Log Files  Reinforcement Learning  Intrusion Detection Systems