عنوان مقاله:

An Effective Approach for Intrusion Detection using Web Mining Techniques

محل انتشار:

دومین کنفرانس ملی رویکردهای نوین در مهندسی کامپیوتر و برق (سال: 1395)

تعداد صفحات اصل مقاله: 5

نویسندگان:

,Masoud Najjar Barghi - *Department of Computer Engineering, Islamic Azad University, Zahedan Branch, Iran*

,Javad Javad - *Department of Computer Engineering, Islamic Azad University, Zahedan Branch, Iran*

خلاصه مقاله:

The Web and its Services are growing rapidly, so is the complexity and the number of cyber-attacks. Thus it is essential to use different security tools in order to protectcomputer systems and networks. Among these tools, Intrusion Detection Systems (IDSs) are one of the components of Defences-in-depth. One major drawback of IDSs is the generation of a huge number of alerts, most of which are false, redundant, or unimportant. Among different remedy approaches, many researchers proposed the use of data mining. Most of the research done in this area could not address the problems completely. Also, most of them suffer from human dependency and offline functionality. In this research, an online approach is proposed in order to manage alerts issued by IDSs. The proposed approach is able to process alerts produced byheterogeneous IDS systems. The approach is evaluated using DARPA 1999 dataset and Shahid Rajaee Port Complex dataset. Evaluation results show that the proposed approach can reduce the number of alerts by 94.32%, effectively improving alert management process. Because of the use of ensemble approach and optimal algorithms in the proposed approach, it can inform network security specialist the state of the .monitored network in an online manner

کلمات کلیدی:

Web Mining Techniques, Intrusion Detection, Fraud Detection

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/522517