عنوان مقاله:

A Survey of Intrusion Alert Correlation Techniques

محل انتشار:

همایش ملی الکترونیکی دستاوردهای نوین در علوم مهندسی و پایه (سال: 1393)

تعداد صفحات اصل مقاله: 10

نویسندگان:

Fatemeh Vafaei Nejad - *Electrical, Computer, and Biomedical Engineering Dep. Qazvin Branch, Islamic Azad UniversityQazvin, Iran*

Behzad Akbari - *Electrical and Computer Engineering Dep.Tarbiat Modares UniversityTehran, Iran*

خلاصه مقاله:

Alert correlation is a significant technique which takes alerts from different Intrusion Detection Systems and reduces redundant and false alerts, extracts high level scenario of attacks, increases the sensitivity of the system and predicts the next adversary’s intention of attacks. In order to reach these aims, many approaches have been introduced with many benefits and drawbacks. In this paper, we prepared an extensive survey on already suggested alert correlation algorithms. The aim of this study is to analyze the current alert correlation approaches and identify the significant challenge and advantage in each technique. The existing alert correlation techniques had been reviewed and analyzed. The result of this survey indicates that each category of alert correlation techniques has its own effectiveness. A perfect alert correlation technique should be took advantage of each category

کلمات کلیدی:

Alert; Alert Correlation; IDS; Network Security; Attack