سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:

Alert Correlation Approach Based on HMM

محل انتشار:

ششمین کنفرانس مهندسی برق و الکترونیک ایران (سال: 1393)

تعداد صفحات اصل مقاله: 8

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 University Tehran, Iran*

خلاصه مقاله:

Huge amounts of low level alerts are daily reported by IDS.Particularly, the large number of which are false positives.A very large quantity of false positives alerts makes it difficult for the security manager to analysis them; thus, in order to cope with such quantities of alerts, alert correlation approaches have been used.In this paper, we describe an architecture for alert correlation based on Hidden Markov Model. Our aim is to reduce the alert redundancy and an extract attack scenario among alerts.An aggregation and correlation module are vital modules of our method. The aggregation module is used to combine the same alerts together. The outcomes of this module are hyper alerts. Afterward, hyper alerts are mapped to the states of the HMM, then the correlation engine estimates the correlation between two hyper alerts among the states. Finally, in order to discover an attack scenario we considered the correlation value between two hyper alerts , so an attack scenario is illustrated by the graph of nodes and edges. The most important point of our approach is that attack scenarios can be detected online without expert knowledge. The efficiency of our proposed approach is evaluated using both the DARPA 2000 dataset and the live traffic data collected from a Honey net network. The experimental results show that the correlation model is effective in achieving .alert reduction and discovering the attack scenario

کلمات کلیدی:

Alert Correlation; Network Security; Attack scenario; Intrusion Detection Systems; Hidden Markov Model

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/383872