Abstract

The increasing number of alerts produced by intrusion detection and monitoring systems in today's networks forces the researchers to apply and further develop the security event management systems in order to secure large scale and critical networks. This Thesis is a study of the security event management system components, focusing on the alert verification part to reduce the amount of alerts investigated by modeling the background noise and detecting abnormal network traffic. Alert correlation components with its three major phases (alert collection, alert aggregation and verification, as well as the high-level alert structures) are studied and investigated, and then the research will focus on the alert verification part in the second phase, which reduces the highest number of alerts.

A variety of researches in this field is developed. A simulation is conducted by modeling the background noise using the Non Stationary time series analysis with lag smoothing Kalman filter, which is inspired from a recent research in this field. Then the implementation and comparison phase follows using a second technique that applies a multi-layered perceptron neural network with back propagation network as a learning algorithm, an approach that is used for the first time in modeling and correlating the background noise. An extracted data flow from DARPA Dataset is used to validate, analyze and compare both techniques. Finally, a verification experiment is conducted on both models using a gathered dataset from real network environment.

ملخص

ازدياد عدد التنبيهات المنبعثة من أجهزة مراقبة و اكتشاف اختراقات الشبكات تدفع الباحثين إلى تطوير و تفعيل أنظمة إدارة تنبيهات إلأمن لتأمين الشبكات الكبيرة و الحيوية.

تحتوي هذه الرسالة على دراسة مكونات نظام أمن إدارة التنبيهات مع التركيز على مكون من هذه المكونات و هو المسؤول عن التحقق من التنبيهات لتقليل كم التنبيهات المكتشفة.

وهذا يتحقق بدراسة تغيرات التنبيهات المهملة ومن ثم اكتشاف انحراف هذه التغيرات عن المسار الطبيعي و المتوقع لها.
يحتوي نظام تجميع و دمج التنبيهات على ثلاث مكونات أساسية:
تجميع و توحيد التنبيهات، التحقق من التنبيهات و أخيرا النظرة الشاملة للتنبيهات لاستنباط الصورة المنظمة لاختراق النظام . لقد تم التركيز على المكون الثاني المسئول عن التحقق من التنبيهات و ذلك لأنه يقلل و يستبعد أكثر عدد من التنبيهات.

لقد تم تطوير كثير من الأبحاث في هذا المجال. لقد تم محاكاه مكون التحقق من التنبيهات عن طريق نمذجة التنبيهات المهملة باستخدام السلسلة الزمنية غير ثابتة التحليل مع استخدام مرشح كالمآنKalman.
هذه المحاكاه مستوحاه من أفضل ما وصلت إليه الأبحاث في هذا المجال.
ثم بعد ذلك تم بناء و مقارنة أسلوب آخر باستخدام الشبكة العصبية متعددة المراحل و خوارزمية التعلم باستخدام شبكة Backpropagation. هذه الطريقة استخدمت للمرة الأولى في نمذجة و دمج التنبيهات المهملة. يتم استخدام تدفق البيانات المستخرجة من مجموعة بيانات دربا DARPA للتحقق، تحليل، و مقارنة الطريقتان. و أخيرا، تم تجربة الطريقتان باستخدام مجموعة بيانات مجمعة من شبكة حقيقية.