بخشی از ترجمه مقاله

عنوان فارسی مقاله :

همبستگی هشدار برای استخراج استراتژی حمله

عنوان انگلیسی مقاله :

Alert Correlation for Extracting Attack Strategies

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل

با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

4.1 Conclusions

Alert correlation is an important technique to aggregate the outputs from multiple IDSs, filter out spurious alerts, and provide a high-level view of the security state of the network. The research in this area is getting active recently because of the fact that generating huge number of alerts has become a major problem of traditional IDSs. A number of correlation approaches have been suggested. However, very few of them provide the capability of automatic extracting attack strategies from alerts. Most of them simply cluster the alerts into different groups.

4.1. نتیجه گیری

همبستگی هشدار یک روش مهم برای متراکم نمودن خروجی ها از چندین IDSs است، هشدارهای جعلی را فیلتر می کند و دید کلی از امنیت شبکه فراهم می آورد. تحقیق در این زمینه اخیرا فعال شده است چون تعداد زیادی از هشدارها به یک مسئله اصلی IDSs مرسوم تبدیل شده است. تعدادی از روش های همبستگی پیشنهاد شده اند. گرچه تعداد کمی از آنها ظرفیت استخراج اتوماتیک استراتژی های حمله از هشدارها را دارند. بیشتر آنها گروه بندی هشدارها را به گروه های متفاوت ساده می سازند.