بخشی از ترجمه مقاله

عنوان فارسی مقاله :

اولویت دهی هشدار نفوذ و کشف حمله با

استفاده از تحلیل Post-Correlation

عنوان انگلیسی مقاله :

Intrusion Alert Prioritisation and Attack Detection using

Post-Correlation Analysis

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

6.2.2. Conclusion

A key observation in the results in both attack scenarios 1 & 2 is that ACSAnIA assigns higher priorities to the alerts which the previous Snort IDSs also prioritised highly. Hence, there is a consistency between both systems. This could be as a result of the following: in both scenarios, highly prioritised alerts have the least frequencies. In a scenario where the vast amount of alerts are supposed to be high priorities, ACSAnIA is unlikely to perform well. This is particularly because ACSAnIA strongly correlates unusual and infrequent activity with higher priorities.

In general, ACSAnIA significantly reduces the volume of alerts a Security Analyst needs to inspect first through correlating alerts into higher level abstract alerts called meta-alerts and then by filtering out low priority meta-alerts. Using the reporting system, a security analyst can explore the clusters and patterns of each meta-alert. Thus, ACSAnIA provides a platform for understanding attack patterns.

6-2-2- نتیجه گیری

یک نظر کلیدی در نتایج در هردو سناریو حمله 1 و2 این است که ACSAnIA اولویت های بالاتر را به هشدارهایی اختصاص می دهد که Snort IDS های قبلی بطور زیاد اولویت بندی میکردند. بنابراین یک سازگاری بین هر دو سیستم وجود دارد. این می تواند به عنوان نتیجه ای که در ادامه می آید باشد: در هر دو سناریو، هشدارهای اولویت بندی شده بالا کمترین تکرار را دارند. در یک سناریو که مقدار زیادی از هشدارها در برتری بالا فرض شده اند، ACSAnIA غیر محتمل است که خوب انجام دهد. زیرا ACSAnIA فعالیت های غیر عادی و کم را شدیدا با برتری بالاتر همبسته می کند.

در کل ACSAnIA به طرز قابل توجهی حجم هشدارها را کاهش می دهد. یک تحلیل امنیتی نیازمند بررسی تمام هشدارهای همبسته در هشدارهای چکیده با سطح بالاتر که meta-alert نامیده می شود و سپس meta-alert های با اولویت پایین را فیلتر می کند. با استفاده از سیستم گزارش دهی، یک تحلیل امنیتی می تواند گروه ها و الگوهای هر meta-alert را کشف کند. بنابراین ACSAnIA یک پایگاه برای تشخیص الگوهای حمله ایجاد می کند.