عنوان مقاله:
بررسی نتایج تحقیقات در زمینه ی کارایی سیستم تشخیص نفوذ Suricata برای امنیت سایبری شبکه های SCADA

محل انتشار:
چهارمین کنفرانس ملی نوآوری و تحقیق در مهندسی برق و کامپیوتر و مکانیک ایران (سال: 1397)

تعداد صفحات اصل مقاله: 12

نویسندگان:
نرجس خاتون کرخی - *دانشجوی کارشناسی ارشد نرم افزار کامپیوتر دانشگاه سبحان نیشابور*

راحله هاشم زهی - *مدرس دانشگاه سبحان نیشابور.*

خلاصه مقاله:
شبکه های کنترل صنعتی SCADA زیرساخت های حیاتی نظیر نیروگاه ها، تاسیسات هسته ای و سیستم های تامین آب را کنترل می کنند. این سیستم ها به طور فزاینده ای هدف حملات سایبری و تهدیداتی از انواع مختلف هستند و حملات موفقیت آمیز به آن ها باعث ایجاد آسیب، هزینه و خسارات جبران ناپذیر می شود. از این رو، نیاز مبرمی به ابزارهای پیشرفته برای تشخیص تهدیدات اینترنتی در شبکه های SCADA وجود دارد. یکی از جدیدترین راهکار های برقراری امنیت و حفاظت از شبکه ها، استفاده از سیستم های تشخیص و پیشگیری از نفوذ می باشد. این مقاله به تعدادی از تلاش ها برای پیشبرد تحقیقات در این زمینه می پردازد. ابتدا سطح پشتیبانی از پروتکل های SCADA در سیستم های شناسایی نفوذ IDS متن باز شناخته شده بررسی و سپس به ارائه ی نتایج تحقیقات انجام شده روی یک IDS خاص به نام Suricata پرداخته شده است. نتایج بررسی های قبلی نشان دهندهی عملکرد بهتر Snort IDS روی سیستم های تک پردازده ای است. این مقاله نشان می دهد در سیستم های چند پردازنده ای، Suricata نسبت به Snort عملکرد بهتری از خود نشان می دهد.

کلمات کلیدی:
لاتین SCADA، امنیت سایبری، IDS، Suricata، پروتکل پروتکل پروتکل

لینک ثابت مقاله در پایگاه سیویلیکا: