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

عنوان مقاله:
یک روش جدید تشخیص و پیشگیری از نفوذ مبتنی بر IPS و IDS

محل انتشار:
دوماهنامه نخبگان علوم و مهندسی, دوره 2, شماره 2 (سال: 1396)

تعداد صفحات اصل مقاله: 12

نویسندگان:
هوشیار مومنه - *دانشجوی ارشد شبکه های کامپیوتری دانشگاه آزاد آشتیان*

عباس کریمی - *دکترای تخصصی کامپیوتر ، استادیار دانشگاه آزاد اراک*

خلاصه مقاله:
سیستم های تشخیص و پیشگیری از نفوذ (IDPS (سیستم های امنیتی ای هستند که برای شناسایی و پیشگیری از تهدیدات امنیتی برای شبکه های کامپیوتری و سیستم های رایانه ای مورد استفاده قرار می گیرند. این سیستم ها به منظور شناسایی و پاسخ خودکار به تهدیدات امنیتی با کاهش خطر در شبکه ها و کامپیوترهای مورد پایش، سازماندهی و طراحی می شوند. سیستم های تشخیص و پیشگیری از نفوذ(IDPS (از روش ها و متد های متعددی نظیر آنالیز های پروتکل چند تراکنشی، امضاء محور و یک سیستم هیبرید بهره می برند که برخی یا همه اجزای سیستم های دیگر را برای شناسایی و پاسخ به تهدیدات امنیتی با هم تلفیق می کنند. رشد سیستم هایی که از ترکیبی از روش ها ایجاد می کنند با انتخاب روش و یا استفاده از سیستم با ابهام و سر درگمی مواجه می شود. هدف این مقاله ارایه یک توجیه کامل از هر روش و پیشنهاداتی جهت بهبود است.

کلمات کلیدی:
سیستم های تشخیص و پیشگیری از نفوذ (IDPS ،(تشخیص ناهنجاری، تشخیص امضاء محور، آنالیز پروتکل چند تراکنشی، تشخیص هیبرید محور

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/643976