

عنوان مقاله:

بررسی کلی در رابطه با سیستم تشخیص نفوذ (IDS) و سیستم پیشگیری از نفوذ (IPS)

محل انتشار:

پنجمین کنفرانس بین المللی مهندسی برق، کامپیوتر و مکانیک (سال: 1400)

تعداد صفحات اصل مقاله: 14

نویسندگان:

هادی بارانی براواتی - دکترای نرم افزار، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی ایران شهر، استادیار دانشکده مهندسی کامپیوتر،
دانشگاه آزاد اسلامی ایران شهر

ندا قدوسیان - دانشجوی کارشناسی نرم افزار، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی ایران شهر

مریم جلالوند - دانشجوی کارشناسی نرم افزار، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی ایران شهر

خلاصه مقاله:

نفوذ در محیط محاسباتی یک فعالیت مخرب ناخواسته بسیار رایج است که از زمان پیدایش منابع محاسباتی ادامه دارد. تعدادی از اقدامات امنیتی برای سه دهه گذشته صورت گرفته است، اما به همان اندازه تهدیدات امنیتی همانند فناوری رشد کرده است. در کل جهان بسته به نوع کامپیوتر، به طور مستقیم یا غیر مستقیم، موضوع بسیار مهم جلوگیری از آن دسته فعالیت ها و تهدیدهای مخربی است که می توانند زیرساخت های محاسباتی را مختل کنند. تشخیص نفوذ سیستم (IDS) و سیستم پیشگیری از نفوذ (IPS) اقدامات استاندارد برای ایمن سازی منابع محاسباتی شبکه هستند. آنها در یک شبکه برای اطمینان از عدم نفوذ در محیط محاسبات مستقر شده اند. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی در میان شبکه حرکت کنید که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش به اهدافی وسوسه انگیز مبدل می شوند، تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند: ۱. سیستم های تشخیص نفوذ (IDS) سیستم های جلوگیری از نفوذ (IPS). تکنولوژی های IDS و IPS ترافیک گذرنده در شبکه را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ریررس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. در مقاله حاضر، این دو فناوری با جزئیات، کارکرد و عملکرد آنها و اثربخشی آنها برای متوقف کردن فعالیت های مخرب در یک شبکه کامپیوتری مورد بحث قرار خواهد گرفت.

کلمات کلیدی:

نفوذ، تشخیص نفوذ، پیشگیری از نفوذ، فایروال، امنیت، IDS ، IPS

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1452390>

