عنوان مقاله:
مقایسه روش های شناسایی سیستم های تشخیص نفوذ (IDS)

محل انتشار:
سومین کنفرانس ملی فناوریهای نوین در مهندسی برق و کامپیوتر (سال: 1398)

تعداد صفحات اصل مقاله: 22

نویسندگان:
فروغ صابری - *دانشجوگروه مهندسی کامپیوتر دانشگاه خلیج فارس بوشهر*

غلامرضا احمدی - *استادراهنما*

خلاصه مقاله:
دستگاه با نرم افزاری که شبکه را برای فعالیت های مخرب یا غیر مجاز نظارت یا شناسایی کند، سیستم تشخیص نفوذ نامیده می شود (IDS). یک اقدام نفوذی ممکن است توسط برخی سیستمها متوقف شود، اما این نه مورد انتظار و نه مورد نیاز سیستم نظارت است. شناخت وقایع ممکن، فهرست کردن اطلاعات در مورد آنها و گزارش محتوای آن است که بر سیستم های تشخیص و پیشگیری از نفوذ متمرکز است (IDPs). سیستم های تشخیص نفوذ ، هر یک از دسترسی غیرمجاز یا سو استفاده از دسترسی به شبکه و منابع کامپیوتر را شناسایی می کند و اساسا یک حمله به این منابع است. مصرف کنندگان باید از حمله مخرب که به طرز فزاینده ای افزایش یافته و آن را می شناسند نگران باشند و نحوه محافظت و اتصال داده های دیجیتال به روشی ایمن تر را به کار ببرند. برای کسب اطلاعات ارزشمند، هکرها از انواع مختلفی از حملات استفاده می کنند که توسط بسیاری از تکنیکهای تشخیص نفوذ، الگوریتم ها و روشها شناسایی می شوند. در این پروژه، سیستم تشخیص نفوذ، طبقه بندی و با انواع تکنیک های تشخیص آن مورد بحث قرار می گیرد.

کلمات کلیدی:
سیستم تشخیص نفوذ، حمله مخرب ، هکرها