عنوان مقاله:
معرفی روشهای فرا ابتکاری برای تشخیص نفوذ و مقایسه آنها

محل انتشار:
دومین همایش چشم انداز تکنولوژی کامپیوتر و شبکه در 2030 (سال: 1395)

تعداد صفحات اصل مقاله: 5

نویسندگان:
جلیل استادعلی اکبری - *دانشجوی کارشناسی ارشد گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران*

کمال میرزایی - *عضو هیات علمی گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران*

محمدضا ملاخلیلی میبدی - *عضو هیات علمی گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران*

خلاصه مقاله:
با مقدار فزاینده شبکه در تهدید امنیت، مطالعه سیستم های شناسایی نفوذ (IDSها) توجه زیادی را در زمینه علم رایانه به خود جلب کرده است. IDS های فعلی چالش هایی را نه تنها برای دسته های نفوذ خرابکارانه بلکه برای قدرت محاسباتی بزرگ نیز مطرح می کند. اگرچه تعدادی از مطالب حاضر در مورد مسایل IDS می باشند، اما ما در تلاش هستیم تا تصویری مفصلتر برای مروری فراگیر ارایه دهیم. هر حمله یا نفوذ خرابکانه ای ممکن است منجر به فجایع جدی شده و سیاست های امنیت رایانه ای را نقض کند. شناسایی نفوذ روند بازرسی رخدادهایی است که در یک سیستم رایانه ای یا شبکه رایانه ای رخ میدهند؛ و تحلیل آنها برای نشانه های نفوذ نیز در آن جای دارد. در این مقاله ، ما روی بررسی و رده بندی روش های مربوط به IDS تمرکز داریم و مقایسه ای کوتاه میان آنها ارایه می دهیم. به منظور مقابله با نفوذگران به سیستم ها و شبکه های کامپیوتری، روش های متعددی تحت عنوان رو شهای تشخیص نفوذ ایجاد گردیده است. یکی از روش های تشخیص مورد استفاده در سیستم های تشخیص نفوذ روش تشخیص رفتار غیرعادی میباشد. تکنیک ها و معیارهایی که در تشخیص رفتار غیرعادی به کارمی روند، عبارتند از :تشخیص سطح آستانه،معیارهای آماری، معیارهای قانو نگرا، سایر معیارها. روشهای فرا ابتکاری در سایر معیارها قرار میگیرند.

کلمات کلیدی:
فرا ابتکاری، تشخیص نفوذ، مقایسه روشها