عنوان مقاله:

بررسی و مقایسه شیوه های تشخیص نفوذ ترکیبی با درنظرگرفتن سطح ریسک در شبکه های کامپیوتری

محل انتشار:

هفتمین همایش بین المللی مهندسی فناوری اطلاعات، کامپیوتر و مخابرات ایران (سال: 1402)

تعداد صفحات اصل مقاله: 12

نویسندگان:

کیمیا محسنیان هروی – دانشجوی کارشناسی ارشد مهندسی سیستم های اطلاعاتی دانشگاه بین المللی امام رضا علیه السلام

حسن شاکری – استادیار گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

خلاصه مقاله:

با رشد روز افزون فناوری اطلاعات و استفاده گسترده از شبکه های کامپیوتری، امنیت شبکه به عنوان یکی از مباحث بسیار مهم و چالش برانگیز این حوزه مطرح است نفوذ در شبکه های کامپیوتری با انگیزه های مختلف، مالی، سیاسی، نظامی و یا برای نشان دادن ضعف امنیتی موجود در برنامه های کاربردی ضعف امنیتی در طراحی شبکه و پروتکل های آن صورت می گیرد. سیستم های تشخیص نفوذ ابزارهای امنیتی هستند که برای تامین امنیت ارتباطات در سیستم های اطلاعاتی مورد استفاده قرار می گیرند. سیستم های تشخیص نفوذ شبکه NIDS (سیستمی که ترافیک ورودی یک شبکه تحلیل میکند) و سیتم های تشخیص نفوذ مبتنی بر هاست HIDS (سیستمی که به فایل های مهم سیستم عامل نظارت می کند). در قسمتی دیگر به الگوریتم های متعددی اشاره شده است که این الگوریتم ها برای رسیدگی به چنین حوزه های پیچیده طراحی شده است .علیرغم مجموعه ای از طبقه بندی های محققان هنوز مکانیزم طبقه بندی قوی را به طور دقیق و سریع در سیستم های تشخیص نفوذ تشخیص نداده اند (که ما در این تحقیق به عملکرد آن ها و نحوه ی جلوگیری از حملات و پیدا کردن راه حل مناسب می پردازیم). از طرف دیگر با توجه به این که در کاربردهای مختلف، میزان ریسک سیستم متفاوت است و همچنین لازم است یک مصالحه بین کارایی و امنیت برقرار شود، بهتر است سیستم تشخیص نفوذ متناسب با سطح ریسک، روال متناسبی برای تشخیص استفاده کند.

کلمات کلیدی:

سیستم تشخیص نفوذ، بد افزار، ریسک، شبکه های کامپیوتری، تشخیص نفوذ ترکیبی.