عنوان مقاله:
ارایه روشی نوین جهت تشخیص نفوذ در شبکه با استفاده از تکنیک های داده کاوی

محل انتشار:
کنفرانس ملی نوآوریهای علوم مهندسی برق (سال: 1396)

تعداد صفحات اصل مقاله: 3

نویسندگان:
رابابه برزگرحاجی آقا - *گروه کامپیوتر ، دانشکده فنی و مهندسی، واحد میانه، دانشگاه آزاد اسلامی، میانه، ایران*

محمدرضا ابراهیمی دیشابی - *گروه کامپیوتر ، دانشکده فنی و مهندسی، واحد میانه، دانشگاه آزاد اسلامی، میانه، ایران*

حامد پزشکی

خلاصه مقاله:
یک نفوذ به عنوان مجموعه ای از فعالیت هایی تعریف می شود که تلاش می کنند یکپارچگی، محرمانگی و در دسترس بودن یک منبع را به مخاطره بیاندازند. یک سیستم تشخیص نفوذ، دسترسی کاربر به سیستم کامپیوتر را با اجرای قوانین خاص، بازبینی و محدود می کند. قوانین، مبتنی بر دانش متخصص می باشد که از مسیولان باتجربه ای که سناریوهای حمله را ساخته اند، استخراج شده است. سیستم، همه ی تخلفات صورت گرفته توسط کاربران را شناسایی کرده و اقدامات لازم برای متوقف کردن حمله روی پایگاه داده را انجام می دهد. مشکل تشخیص نفوذ در امنیت کامپیوتر به طور وسیعی بررسی شده است. سیستم تشخیص نفوذ، نرم افزار یا سخت افزاری است که عمل تشخیص نفوذ را به طور خودکار انجام می دهد. با روند رو به رشد استفاده از شبکه های کامپیوتری به خصوص اینترنت و مهارت رو به رشد کاربران و مهاجمان این شبکه ها و نیز نقاط آسیب پذیری مختلف در نرم افزارها، ایمن سازی سیستم ها و شبکه های کامپیوتری از اهمیت بیشتری نسبت به گذشته برخوردار شده است. تامین امنیت در هر سیستم یا شبکه ی کامپیوتری می تواند به دو صورت، یکی از طریق پیشگیری امنیتی و دیگری از طریق تشخیص تخطی از سیاست های امنیتی انجام پذیرد. روش های مختلفی برای تشخیص نفوذ در سیستم پیشنهاد شده است. در این میان روش هایی که از داده کاوی و یادگیری ماشین استفاده می کنند، مورد توجه هستند. [1] در این تحقیق به دنبال ارایه ی روشی دو مرحله ای هستیم. در لایه ی اول سعی داریم تا با استفاده از روش های خوشه بندی، مجموعه داده را خوشه بندی کرده و سپس در لایه دوم داده های نرمال را از غیر نرمال تششخیص دهیم. لایه ی اول باعث ساده سازی می شود زیرا هم حجم داده را کاهش داده و هم باعث تمرکز دسته بند برروی داده های جمع آوری شده در لایه ی دوم می شود.

کلمات کلیدی:
سیستم تشخیص نفوذ، دسته بندی، یادگیری ماشین، داده کاوی