عنوان مقاله:
استفاده از داده کاوی جهت بهبود تشخیص نفوذ در شبکه های Server Based

محل انتشار:
سومین همایش ملی فناوریهای نوین در صنایع برق و رباتیک (سال: 1394)

تعداد صفحات اصل مقاله: 10

نویسندگان:
محسن شکیبا فخر - *آموزش کل فنی و حرفه ای سما، دانشگاه آزاد اسلامی واحد شوشتر*

ساسان سفاییان - *آموزشکده فنی و حرفه ای سما، دانشگاه آزاد اسلامی واحد شوشتر*

مجتبی خیاط - *آموزشکده فنی و حرفه ای سما، دانشگاه آزاد اسلامی واحد شوشتر*

خلاصه مقاله:
تشخیص نفوذ عبارتست از تشخیص تلاش هایی که جهت دسترسی غیرمجاز به یک شبکه با کاهش کارایی آن انجام می شوند. برای ایجاد امنیت کامل در یک سیستم کامپیوتری علاوه بر دیواره های آتش و دیگر تجهیزات جلوگیری از نفوذ، سیستم های دیگری به نام سیستم های تشخیص نفوذ IDS مورد نیاز می باشند تا بتوانند در صورتی که نفوذ گر از دیواره های آتش، آنتی ویروس و دیگر تجهیزات امنیتی عبور کرد و وارد سیستم شد آن را تشخیص داد و چاره ای برای مقابله با آن بیندیشد. در این مقاله با الگو نمودن رفتارهای نرمال یک شبکه کامپیوتری و ایجاد نماهای رفتاری آن، هر گونه تجاوز و تخطی از این رفتارهای نرمال به عنوان نفوذ احتمالی تشخیص داده شده و به اطلاع مسئول امنیتی سیستم رسانده می شود. ایجاد این الگوها به روش داده کاوی می باشد. بدین صورت که با محاسبه ویژگی های رفتاری شبکه، اقدام به پیدا کردن ارتباط بین این ویژگی ها نمود و با ایجاد قوانینی بر اساس این ارتباطات، رفتارهای شبکه را به عنوان رفتارهای نرمال آن شبکه مدل می نماییم و بر اساس این رفتارها به شناسایی رفتارهای غیر نرمال می پردازیم.

کلمات کلیدی:
کشف نفوذ ، داده کاوی، ترافیک نفوذی، رفتار نرمال

لینک ثابت مقاله در پایگاه سیویلیکا: