عنوان مقاله:
ارائه یک معماری جدید برای استفاده از داده کاوی در طرحی سیستم های تشخیص نفوذ

محل انتشار:
سومین همایش ملی کامپیوتر (سال: 1394)

تعداد صفحات اصل مقاله: 8

نویسندگان:
امین امیدی قاسم آباد - *دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد رشت*

هادی ویشکی نژاد - *دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد رشت*

سیده حورا فخر موسوی - *هیات علمی دپارتمانمهندسی کامپیوتر دانشگاه آزاد اسلامی لاهیجان گیلان ایران*

خلاصه مقاله:
دراین مقاله راه های نفوذبه شبکه های کامپیوتری و روشهای مقابله با آنها معرفی میگردد سیستم های تشخیص نفوذی که براساس داده کاوی طراحی شدها ند درشبکه های کوچک و محلی دارای عملکردبسیارخوبی هستند ولی درشبکه های بزرگ بدلیل تولید هشدارهای اشتباه و منفی درزمینه حملات به شبکه عملادارای کاربرد نیستند به همین دلیل دراین سیستم ها عملا ازداده های کاوی استفاده نمی کنند درسیستم های تجاری ازالگوی و امضای حملات شناخته شده استفاده میگردد که به آن امضاهای ایستا گویند این بدان معناست که امضا و الگوی هرحمله پس ازمشاهده رفتارآن حمله و ثبت داده های مربوط به ان با تحلیلهایی که برروی داده ها صورت میگیرد تهیه میگردد بدین وسیله سیستم درایننده به راحتی آن حمله را خواهد شناخت و جلوی نفوذ و حمله به شبکه را خواهد گرفت امروزه برای تحلیل برروی داده ها جهت استخراج امضا ازداده کاوی استفاده میگردد دراین مقاله با تعریف نفوذ و داده کاوی به بررسی کاربردهای داده کاوی درتشخیص نفوذ می پردازیم و دراخرمعماری پیشنهادی را بیان کرده و سپس شرح میدهیم

کلمات کلیدی:
نفوذ ، سیستم های تشخیص نفوذ ، پشتیبان ، آسیب پذیری ، داده کاوی