عنوان مقاله:
روش لایه ای با استفاده از ماشین های بردار پشتیبان برای تشخیص نوع ناهنجاری ها در تشخیص نفوذ

محل انتشار:
کنگره ملی مهندسی برق، کامپیوتر و فناوری اطلاعات (سال: 1392)

تعداد صفحات اصل مقاله: 7

نویسندگان:
زینب ابویی مهریزی - *دانشگاه صنعتی اصفهان، دانشکده برق*

سیدرسول موسوی - *دانشگاه صنعتی اصفهان، دانشکده برق*

مهدی برنجکوب - *دانشگاه صنعتی اصفهان، دانشکده برق*

محسن نوروزی

خلاصه مقاله:
سیستم های تشخیص نفوذ) – IDS (دارای چالش های زیادی هستند. از جمله این سیستم ها باید قادر باشند با حجم زیاد داده ها کار کنند. مهاجمان روز به روز سعی در شکستن امنیت دارند و هر روز حملات جدیدترکشف می شوند. از این رو سیستم های تشخیص نفوذ، پس از مدتی کارایی خود را از دست می دهند و قادر به تشخیص حملات جدید نیستند. وقتی IDS ها نشانی از نقض امنیت پیدا کنند، هشدار یا هشدارهایی را تولید می کنند. اماآن ها روزانه تعداد بسیار زیادی هشدار تولید می کنند که بسیاری از این هشدارها مربوط به فعالیت های عادی هستند. ما در این مقاله روشی را پیشنهاد کردیم که هشدارهای تولید شده توسط IDS ها را به پنج کلاس R2L ، Probe ، DoS، Normal و U2R تقسیم می کند. روش پیشنهادی از چندین لایه تشکیل شده که هر لایه قادر به شناسایی یکی از حملات R2L ، Probe ، DoS وU2R است و در هر لایه از روش SVM برای دسته بندی حملات استفاده شده است. برای این که سیستم پیشنهادی پس از گذشت زمان کارایی خود را از دست ندهد، به صورت خودکار و با کمک گرفتن از تحلیل گر سیستم، به روز می شود . این روش دارای نرخ تشخیص بالایی در شناسایی حملات است. نتایج روش پیشنهادی با روش لایه ای CRF مقایسه شده است، که نتایج حاکی از این است که روش پیشنهادی در تشخیص حملات R2L ، DoS و U2R دقیق تر است

کلمات کلیدی:
تشخیص نفوذ، روش مبتنی بر لایه، ماشین های بردارپشتیبان، آموزش افزایشی، Conditional Random Field ، امنیت شبکه