9th SASTech Symposium on Advances in Science & Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
با محوریت
امنیت ملی و توسعه پایدار
برگزار کننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

مروری بر سیستم‌های تشخیص نفوذ با استفاده از ماشین بردار پشتیبان

نرگس صالح پور[۱]، دکتر سیروس مرادی[۲]، محمد نظری فرخی[۳]

[۱]دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی واحد خرم آباد
[۲]عضو هیات علمی، گروه ریاضی، دانشگاه آزاد اسلامی اراک
[۳]دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی واحد خرم آباد

Salehpour_narges@yahoo.com
نام ارائه‌دهنده: نرگس صالح پور

خلاصه

امروزه با رشد کاربران اینترنت، نفوذ به سیستم‌های کامپیوتری از طریق شبکه نیز در حال افزایش است. بدین منظور امنیت شبکه به‌عنوان یک مسئله‌ی جدی برای کاربران به شمار می‌رود. بنابراین سیستم‌های تشخیص نفوذ برای کشف و شناسایی حملات و تشخیص اشکالات امنیتی در شبکه‌های کامپیوتری مورداستفاده قرار می‌گیرند. ماشین بردار پشتیبان نیز به‌عنوان نمونه‌ای از تکنیک‌های داده‌کاوی در سیستم‌های تشخیص نفوذ به شمار می‌رود. بدین‌وسیله الگوریتم تشخیص الگو حملات را شناسایی و دسته‌بندی می‌کند. هدف استفاده از ماشین بردار پشتیبان، انتخاب بهترین تفکیک کننده خطی است که خطای تعمیم را به حداقل می‌رساند. اما در تکنیک ماشین بردار پشتیبان به زمان آموزشی نسبتاً بالایی نیاز خواهد بود. بنابراین بهتر است، از روش‌های ترکیبی ماشین بردار پشتیبان با دیگر تکنیک‌های داده‌کاوی در مجموعه داده‌ی UNM به‌منظور تسریع در تشخیص نفوذ شبکه‌های کامپیوتری استفاده شود.

کلمات کلیدی: سیستم‌های تشخیص نفوذ، داده کاوی، شبکه‌های عصبی، ماشین بردار پشتیبان، هوش محاسباتی

۱. مقدمه

امروزه کامپیوتر و شبکه‌های کامپیوتری متصل به اینترنت نقش عمده‌ای در ارتباطات و انتقال اطلاعات ایفا می‌کنند. در این میان افراد سودجو با دسترسی به اطلاعات مهم قصد نفوذ و به هم ریختن نظم سیستم‌ها را در پیش‌گرفته‌اند. هک، کرک و نفوذ، اصطلاحاتی هستند که امروزه در شبکه‌های کامپیوتری ازجمله خطرات نفوذ به شبکه‌های کامپیوتر می‌باشند که منجر به محرومیت از خدمات وب می‌شوند. امنیت شبکه‌های کامپیوتری یکی از مکانیسم‌های تشخیص نفوذ است که برای کشف دسترسی‌های غیرمجاز شبکه در تلاش است. ازجمله دسترسی‌های غیرمجاز و فعالیت‌های مخرب مانند حملات ویروس، دسترسی غیرمجاز و سرقت اطلاعات را مورد تجزیه‌وتحلیل قرار می‌دهند. البته در چند سال اخیر امنیت سایبری نیز موردتوجه قرارگرفته است. ابتدا فایروال‌ها تنها خط دفاع برای امنیت شبکه‌های کامپیوتری بودند. با توجه به آمار، از سال ۲۰۰۰ تا ۲۰۰۷ استفاده‌کنندگان از اینترنت به بیش از یک میلیارد می‌رسید. با توجه به این امر که امروزه تعداد کاربران اینترنت تا ۲۱۴ درصد رشد داشته است که البته همراه با رشد کاربران اینترنت، نفوذ به سیستم‌های کامپیوتری نیز از طریق شبکه در حال افزایش است. بنابراین امنیت شبکه به یک مسئله جدی برای کاربران شخصی و شرکت‌های بزرگ تبدیل‌شده است. به‌طورکلی امنیت شامل آنتی اسپم، آنتی‌ویروس، ورود و خروج، حسابرسی‌ها و فایروال‌ها می‌باشد که آنتی اسپم نیز بر روی کاربران نهایی تمرکز دارد و ایمیل‌هایی که در اسپم قرار می‌گیرند را مسدود می‌کند. تکنیک‌های ضدویروس نیز معمولاً برای شناسایی نرم‌افزار، بلوک و از بین بردن ویروس‌های کامپیوتری و برنامه‌های مخرب استفاده می‌شوند. هدف از تشخیص نفوذ به‌ظاهر ساده است اما با این‌حال کار سختی است و در همه‌ی سیستم‌های کامپیوتری فقط شواهدی از نفوذ قابل شناسایی است. این شواهد گاهی به‌عنوان حمله جلوه می‌نمایند.