تشخیص نفوذ شبکه های کامپیوتری

Computer network interusion detection

مولفان:

مهندس سیده مریم حسینی

دانشگاه آزاد اسلامی واحد تهران شمال

دکتر ناصر مدیری

دانشگاه آزاد اسلامی واحد زنجان

عنوان: تشخیص نفوذ شبکه های کامپیوتری

مولف:مهندس سیده مریم حسینی– دکتر ناصر مدیری

ناشر:سنجش و دانش

نوبت چاپ: اول–۱۳۹۹

تیراز: ۵۰۰ نسخه

شابک:۰–۱۱۳۸–۰۵–۶۲۲–۹۷۸

نشانی: میدان انقلاب. خیابان انقلاب. خیابان دانشگاه. پلاک ۱۲۶.

تلفن:۰۲۱۶۱۲۶

www.sanjesh.ir

sanjeshodanesh@iran.ir

قیمت:۳۵۰۰۰۰ریال

ISBN:9[illegible]22-05-1138-0

9 786220 511380

فهرست مطالب

پیشگفتار:

با رشد فناوری اطلاعات امنیت، شبکه به عنوان یکی از مباحث مهم و چالش بسیار بزرگ مطرح است. سیستم های تشخیص نفوذ مولفه اصلی یک شبکه امن است. سیستم های تشخیص نفوذ سنتی نمی توانند خود را با حملات جدید تطبیق دهند از این رو سیستم های تشخیص نفوذ مبتنی بر داده کاوی امروزه پیشنهاد می شود. مشخص نمودن الگوهایی در حجم زیاد داده، کمک بسیار بزرگی به ما می کند. متدهای داده کاوی با مشخص نمودن یک برچسب دودویی (بسته نرمال، بسته ناهنجار) و همچنین مشخص نمودن ویژگی ها و خصیصه با الگوریتم های دسته بندی می توانند داده غیرنرمال را تشخیص دهند. از همین رو دقت و درستی سیستم های تشخیص نفوذ افزایش یافته و سطح امنیت شبکه بالا می رود. در این روش ما الگوریتم های مختلف شبکه و شبکه عصبی را روی مجموعه داده خود تست خواهیم کرد.امروزه تهدیداتی که از اینترنت می‌آیند بیش از پیش پیچیده شده و توانایی این را دارند که از راه‌حل‌های امنیتی معمول از قبیل دیوار آتش‌ها و آنتی ویروس ها عبور کنند. یک راه حل ممکن برای بهبود امنیت، اضافه کردن یک سیستم تشخیص نفوذ است که بعنوان یک لایه اضافی در راه‌حل‌های امنیتی محسوب میشود. هدف از تشخیص نفوذ، شناسایی فعالیت هایی است که قصد استفاده غیرمجاز، آسیب رساندن به سیستم‌ها وسوءاستفاده از شبکه‌های کامپیوتری را دارند. در این میان، روش‌های متعددی توسط محققین ارائه شده است که هریک به نوبه خود عملکرد خوبی رو به رشدی داشته‌اند. اما با توجه به حجم عظیم داده‌ها در هر سازمان مبتنی بر شبکه، مثل شبکه‌های مخابراتی، بررسی و تحلیل ترافیک موجود به صورت دستی کاری دشوار، کم دقت و زمانبری است. با این وجود با بهره گیری از تکنیک‌های دسته‌بندی در زمینه داده‌کاوی با استفاده از شبکه عصبی و الگوریتم ژنتیک می‌توان به تحلیل خودکار و تشخیص امنیت شبکه پرداخت.