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
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

بررسی سیستم های تشخیص نفوذ مبتنی بر شبکه های عصبی نظارت نشده

رضا خدابنده لو ،مجید خلیلیان

دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی بویین زهرا

استاد دانشگاه آزاد اسلامی کرج

taninrayaneh@yahoo.com

چکیده

در حوزه شبکه ،امنیت ،کنترل دسترسی و تشخیص به موقع با دقت بالا از ترافیک شبکه از مباحث میباشد.عملا هیچ سیستمی امنیت کامل ندارد.سیستم IDSبرای تشخیص نفوذ به موقع در ساختار شبکه بسیار جای خود را با ز کرده و نیاز اساسی در شبکه ای میباشد .در این میان محققان به دنبال روش های مختلف برای بر آورده کردن این نیاز به کشف و طراحی انواع سیستم های خبره ،تغییر گذر حالات ،شبکه پتری ،روشهای آماری ،داده کاوی و شبکه های عصبی می باشد .روشهای IDSشبکه های عصبی به دو دسته ۱- با ناظر مانند پیشخور چند لایه ،بازگشتی و ۲- بدون ناظر مانند همینگ ،کوهنن و Artتقسیم می شوند .مزیت شبکه های عصبی بدون ناظر در این است که حملات شناخته نشده جدید را نیز می تواند شناسایی کند و نیاز به آموزش مجدد ندارند .در این مقاله چند روش شبکه های عصبی بدون ناظر مورد بررسی قرار می دهیم .

کلید واژه :شبکه های عصبی نظارت شده ،KDD CUPشبکه های عصبی SOM وART

۱–مقدمه

گسترش روز افزون ارتباطات کامپیوتری وترافیک ایجاد شده تامین امنیت در برابر حملاتی نظیر دستکاری اطلاعات ، افزودن اطلاعات، استراق سمع ، قطع ارتباط کاربر DOSیاDDOS با استفاده از IP واطلاع از پورت های باز امری اجتناب ناپذیر می باشد. باتوجه به نفوذ هکرها از دیواره آتش وحتی ویروس یاب ها ، IDS ها ابزاری مناسب جهت تشخیص نفوذ واعلام هشدارها به مدیر شبکه می باشد.راههای نفوذ به کامپیوتر میزبان یا شبکه ویا به صورت ترکیبی وتوامان به دسته های زیر تقسیم می شوند:

حمله از طریق IP،حمله به TCP،جعل اطلاعات ،حمله به کلمات عبور ،حمله به برنامه های کاربردی ،استراق سمع(sniffer)،حملات اختلال در سرویس دهی،قطع ارتباط باDOS وDDOS ،ویروس ها واسب تروا ،پورت های باز(عبور بدون مرز)،حمله به سیستم عامل(ROOT KIT).

مقابله با نفوذ در دو سطح زیر انجام می گیرد:

۱-کنترل واعتبارسنجی

۲-سیستم های IDS

مادر این مقاله از سطح دوم استفاده می کنیم وبه تشریح انواع مختلف شبکه های عصبی نظارت نشده می پردازیم.

اهداف IDS :

۱-تشخیص گستره وسیعی از حملات

۲-تشخیص نفوذ به موقع

۳-تجزیه وتحلیل سریع وآسان

۴-به حداقل رساندنFNRو PPR [5]

استفاده از شبکه های عصبی باعث میشود دسته بندی خوب،تعمیم پذیری بالا،انعطاف پذیری،سرعت مناسب،کاهش نرخ اعلان خطا داشته باشیم.

روشهای تشخیص نفوذ به شبکه های کامپیوتری به دو دسته تقسیم میشوند: