بهبود عملکرد سیستم‌های اشکال‌یاب نفوذ در شبکه‌های رایانه‌ای

با استفاده از روش مرکب

مؤلف:

سید حمیدرضا اعرابی

سرشناسه : اعرابی، سید حمیدرضا، ۱۳۶۰ -
عنوان و نام پدیدآور : بهبود عملکرد سیستم‌های آشکارساز نفوذ در شبکه‌های رایانه‌ای با استفاده از روش ترکیبی/ مولف سید حمیدرضا اعرابی.
مشخصات نشر : تهران: سنجش و دانش، ۱۳۹۸.
مشخصات ظاهری : ۱۵۸ص.
شابک : 978-622-050889-2
وضعیت فهرست نویسی : فیپا
یادداشت : واژه‌نامه.
یادداشت : کتابنامه: ص.۱۰۵.
موضوع : سامانه‌های تشخیص نفوذ (ایمن‌سازی کامپیوتر) -- ایران -- نمونه‌پژوهی
موضوع : Intrusion detection systems (Computer security) -- Iran -- Case studies
موضوع : شبکه‌های کامپیوتری -- ایران -- تدابیر ایمنی -- نمونه‌پژوهی
موضوع : Computer networks -- Iran -- Security measures -- Case studies
رده بندی کنگره : TK۵۱۰۵/۵۹
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۴۹۹ ۴۰۴

عنوان: بهبود عملکرد سیستم‌های آشکارساز نفوذ در شبکه‌های رایانه‌ای با استفاده از روش ترکیبی

مولف: سید حمیدرضا اعرابی

ناشر: سنجش و دانش

نوبت چاپ: اول-۱۳۹۸

تیراژ: ۵۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۰۵-۰۸۸۹-۲

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

تلفن: ۰۲۱۶۱۲۶

سنجش و دانش

www.sanjesh.ir

sanjeshodanesh@iran.ir

قیمت: ۲۵۰۰۰۰ ریال

ISBN:978-622-05-0889-2

پیش‌گفتار مؤلف :

نقش یک سیستم تشخیص نفوذ برای آشکارسازی ناهنجاری‌ها در شبکه از اهمیت زیادی برخوردار است. حملات جدید و ناشناخته موجب ناکارآمدی راه‌کارهای شناسایی مبتنی بر امضاء و در نتیجه استفاده از راه‌کارهای شناسایی مبتنی بر ناهنجاری شده است. این راه‌کارها نیز علی‌رغم توانایی بالا در تشخیص ناهنجاری‌ها، از نرخ مثبت کاذب بالایی رنج می‌برند. برای غلبه بر این مشکل، ایده استفاده از آشکارسازهای ترکیبی مطرح‌شده است. در این پژوهش راه‌کاری نوین مبتنی بر روش آشکارسازی ترکیبی با یک معماری چهارلایه‌ای پیشنهادشده است. لایه‌ی اول از ماژول تحلیل‌گر جریان داده‌ها و ماژول طبقه‌بندی تشکیل‌شده است که برای طبقه‌بندی نوع سرویس‌های شبکه از ترکیب تکنیک آماری n-گرام و الگوریتم ژنتیک استفاده می‌کند. در لایه‌ی تشخیص نفوذ، یک ماژول آشکارساز مبتنی بر امضاء و ماژول‌های آشکارساز مبتنی بر ناهنجاری به شکل ترکیبی پیاده‌سازی شده‌اند که متناسب با برچسب نوع سرویس‌ها فراخوانی می‌شوند. سپس درنتیجه‌ی پردازش این ماژول‌ها، لایه تصمیم‌گیری فراخوانی می‌شود. این لایه ماهیت حمله و نوع پاسخ را تشخیص داده و لایه‌ی مدیریت وقایع را فرامی‌خواند. در این لایه ضمن اطلاع‌رسانی هشدارها به مدیر شبکه، در صورت نیاز اعمال واکنشی و اقدامات امنیتی لازم نیز انجام خواهد شد. نتایج حاصل از ارزیابی اعتبارسنجی چهارلایه‌ای، بهبود دقت تشخیص نفوذ را ۹۹.۸۱ درصد نشان می‌دهد که درنتیجه کاهش میزان نرخ مثبت کاذب را در پی خواهد داشت.هدف از این پژوهش کاهش نرخ مثبت کاذب در تشخیص نفوذ در شبکه است. اهمیت موضوع در تشخیص دقیق‌تر نفوذ در شبکه است. روش پیشنهادی مبتنی بر ادغام دو روش شناخته‌شده، مبتنی بر امضاء و مبتنی بر ناهنجاری در ترافیک شبکه است. برای کاهش نرخ مثبت کاذب با شناسایی و طبقه‌بندی سرویس‌های ترافیک شبکه بر اساس برچسب نوع سرویس‌ها می‌توان مدل‌های مناسب که با داده‌های مربوط به هر نوع سرویس به‌طور مجزا آموزش‌دیده‌اند را برای تشخیص نفوذ مورداستفاده قرارداد. در صورت عدم شناسایی نوع سرویس از جریان داده ترافیک شبکه می‌بایست مدل‌های موجود را با مجموعه داده‌های آموزشی به‌روز بررسی کرد. روش‌های مبتنی بر امضاء نیازمند بروز رسانی مکرر پایگاه داده حملات در فواصل زمانی کوتاه هستند. بعلاوه حملاتی که از روش‌های رمزنگاری داده‌ها استفاده می‌نمایند توسط این روش به‌سختی قابل‌تشخیص هستند. در این روش، الگوهای نفوذ از پیش‌ساخته (امضاء) به‌صورت الگوهای حمله نگهداری می‌شوند، به‌طوری‌که هر الگو انواع متفاوتی از یک نفوذ خاص را در بر گرفته و در صورت بروز

چنین الگویی در سیستم، وقوع نفوذ اعلام می‌شود. در این روش‌ها، معمولاً تشخیص‌دهنده دارای پایگاه داده‌ای از امضاءها یا الگوهای حمله است و سعی می‌کند با بررسی ترافیک شبکه، الگوهای مشابه با آنچه را که در پایگاه داده‌ی خود نگهداری می‌کند، بیابد. این دسته از روش‌ها تنها قادر به تشخیص نفوذهای شناخته‌شده می‌باشند و در صورت بروز حملات جدید در سطح شبکه، نمی‌توانند آن‌ها را شناسایی کنند و نیازمند بروز رسانی پایگاه داده‌ای[1] از امضاءها یا الگوهای حمله در فواصل زمانی کوتاه هستند. در این روش نرخ مثبت کاذب پایین است و از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آن‌ها قبلاً شناسایی و در پایگاه داده‌ها ثبت شده است.روش آشکارسازی ناهنجاری به این صورت است که بر اساس داده‌های طبیعی مدل‌هایی از فعالیت‌های قانونی ساخته شده و در صورت انحراف از مدل مذکور حمله یا ناهنجاری در نظر گرفته و برای رسیدن به این هدف دو فاز در نظر گرفته می‌شود، فاز آموزش و فاز آزمایش، در فاز آموزش با استفاده از تکنیک‌های یادگیری ماشین بر اساس داده‌های آموزشی مدل طبیعی[2] ساخته می‌شود. در فاز آزمایش مدل یاد گرفته‌شده در برابر نمونه‌های جدید با استفاده از داده‌های آموزشی که از قبل ساخته شده‌اند آزمایش می‌شود. بر همین اساس این نوع آشکارسازها توانایی تشخیص حملات ناشناخته و جدید را دارند. هدف دیگر از این پیشنهاد، ارائه روشی کارآمد با هزینه‌ی کمتر به‌منظور تشخیص فعالیت‌های نفوذگرانه است. روش پیشنهادی سعی در افزایش دقت تشخیص آشکارسازها و کاهش نرخ مثبت کاذب نسبت به سایر روش‌های دیگر را دارد. این کار از طریق بررسی معایب روش‌های تشخیص نفوذ و بررسی راه‌کارهای نظام‌مند سازی فرآیند تشخیص نفوذ با استفاده از مدل‌های یادگیری ماشین و باهدف ارائه روشی جدید بر اساس روش‌های طبقه‌بندی و تشخیص محقق می‌گردد.در آشکارسازهای مبتنی بر امضاء نرخ مثبت کاذب پایین است و آشکارسازهای ناهنجاری در تشخیص حمله‌های شناخته‌شده و ناشناخته توانایی بالایی دارند. در روش آشکارسازی ناهنجاری دو چالش عمده وجود دارد. چالش اول پیاده‌سازی یک ماژول تحلیل‌گر برای طبقه‌بندی نوع سرویس ترافیک شبکه با دقت بالا است. چنانچه این بخش به‌درستی انجام گیرد، خروجی‌های به دست آمده در مراحل بعد نیز تأثیرگذار خواهند بود؛ و در نهایت علی‌رغم توانایی بالا در تشخیص آسیب‌پذیری‌های ناهنجاری، این روش از میزان بالای نرخ مثبت کاذب رنج می‌برد بنابراین چالش دیگر، در مرحله تشخیص ماهیت و نوع حمله است. روشی مناسب است که علاوه بر تشخیص تعداد بیشتر حملات نسبت به

---

[1] Data Base
[2] Normal Model

روش‌های دیگر، بتواند نرخ مثبت کاذب کمتری داشته باشد .در این پژوهش سیستمی مبتنی بر روش ترکیبی معرفی‌شده استفاده شده است. به‌این‌ترتیب به‌طور هم‌زمان از نرخ آشکارسازی بالای حملات شناخته‌شده در دسته اول و توانایی آشکارسازی حملات ناشناخته و جدید در دسته دوم، بهره‌مند می‌شویم. در بین تکنیک‌های مختلف امنیتی در شبکه‌های کامپیوتری، نقش سیستم‌های آشکارسازی نفوذ (IDS) به‌عنوان عاملی برای تشخیص ناهنجاری‌ها و حملات، از اهمیت بسیار بالایی برخوردار است. راه‌کار پیشنهادی از چهار لایه : ۱. لایه تحلیل و طبقه‌بندی ترافیک شبکه ۲. لایه تشخیص نفوذ ۳. لایه تصمیم‌گیری ۴. لایه مدیریت ثبت وقایع و هشدارها تشکیل شده است که نتیجه این پژوهش بهبود عملکرد سیستم‌های آشکارساز نفوذ را نشان می‌دهد.

بی‌شک هر اثر علمی بدون ایراد نبوده و از خوانندگان و اساتید محترم تقاضا می‌شود که نظرات و دیدگاه‌های ارزشمند خود را به صندوق الکترونیکی aarabihamidreza@gmail.com ارسال نمایند.

به امید اینکه این خدمت ناچیز مورد قبول درگاه الهی قرار گیرد.

سید حمیدرضا اعرابی

آبان ماه ۱۳۹۷