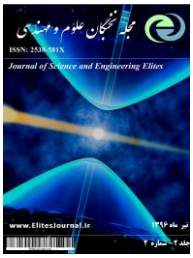
مجله نخبگان علوم و مهندسی
Journal of Science and Engineering Elites
ISSN 2538-581X
جلد ۲- شماره ۲- سال ۱۳۹۶
www.ElitesJournal.ir



یک روش جدید تشخیص و پیشگیری از نفوذ مبتنی بر IPS و IDS

هوشیار مومنه[۱*]، عباس کریمی[۲]

۱-دانشجوی ارشد شبکه های کامپیوتری دانشگاه آزاد آشتیان

۲- دکترای تخصصی کامپیوتر ، استادیار دانشگاه آزاد اراک

*hoshyarm@yahoo.com

ارسال: اردیبهشت ماه ۹۶ پذیرش: تیر ماه ۹۶

چکیده

سیستم های تشخیص و پیشگیری از نفوذ (IDPS) سیستم های امنیتی ای هستند که برای شناسایی و پیشگیری از تهدیدات امنیتی برای شبکه های کامپیوتری و سیستم های رایانه ای مورد استفاده قرار می گیرند. این سیستم ها به منظور شناسایی و پاسخ خودکار به تهدیدات امنیتی با کاهش خطر در شبکه ها و کامپیوترهای مورد پایش، سازماندهی و طراحی می شوند. سیستم های تشخیص و پیشگیری از نفوذ(IDPS) از روش ها و متد های متعددی نظیر آنالیز های پروتکل چند تراکنشی، امضاء محور و یک سیستم هیبرید بهره می برند که برخی یا همه اجزای سیستم های دیگر را برای شناسایی و پاسخ به تهدیدات امنیتی با هم تلفیق می کنند. رشد سیستم هایی که از ترکیبی از روش ها ایجاد می کنند با انتخاب روش و یا استفاده از سیستم با ابهام و سر درگمی مواجه می شود. هدف این مقاله ارایه یک توجیه کامل از هر روش و پیشنهاداتی جهت بهبود است.

کلمات کلیدی: سیستم های تشخیص و پیشگیری از نفوذ (IDPS)، تشخیص ناهنجاری، تشخیص امضاء محور، آنالیز پروتکل چند تراکنشی، تشخیص هیبرید محور.

۱. مقدمه

سیستم های تشخیص و پیشگیری از نفوذ (IDPS)، تبدیل به یک ابزار ارزشمند در حفظ و ایمن سازی سیستم های اطلاعاتی شده اند. این سیستم ها ابزارهای امنیتی هستند که برای پایش، تجزیه، تحلیل و پاسخ به تناقضات و مشکلات امنیتی در برابر سیستم های شبکه و کامپیوتر مورد استفاده قرار می گیرند. این تجاوزات می توانند ناشی از شکست و نفوذ در نفوذهای خارجی غیر مجازی باشند که تلاش می کنند تا سیستم را با مشکل مواجه سازند و یا از کاربران مجاز داخلی و هویت آنها سوءاستفاده کنند. روش های مهم و سودمند به طور هم زمان و سرعت مشابه ایجاد نشده و کمتر نیز با روش های دیگر ترکیب و تلفیق می شوند.

با توجه به اهمیت بالای امنیت در شبکه ها و تلاش در جهت کاهش آسیب پذیری و روشهای بروز نفوذ، امروزه دنیا شاهد چالشهای بزرگی در این مساله می باشد و می بایست بصورت لحظه ای با روشهایی جدید و کارآمد آماده مقابله با هرگونه تهدید و نفوذ باشد و راهکارهای جدید و متنوعی برای تشخیص و پیشگیری از نفوذ داشته باشد.

به همین منظور موضوع تشخیص و پیشگیری از نفوذ می تواند همواره موضوعی جهت بررسی و ارائه راه کارهای نوین و جدید باشد. در این مقاله سعی بر بررسی راهکارها و متدهای مختلف ارائه شده در رابطه با موضوع تشخیص و پیشگیری از نفوذ مبتنی بر IPS و IDS صورت خواهد گرفت.

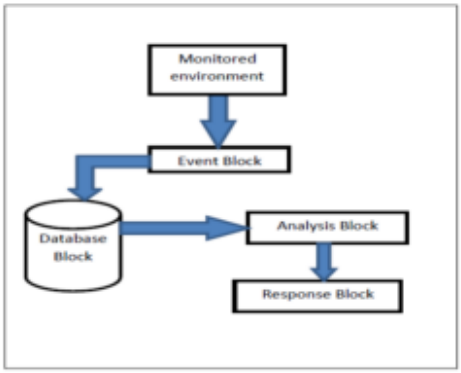
۲. مروری بر مطالعات پیشین

پیشگیری از نفوذ ناشی از مطالعات انجام شده بر روی موانع و محدودیت های تشخیص نفوذ است. تشخیص نفوذ از گزارش هایی برگرفته شده است که یک مدل تهدید را پیشنهاد می دهند [۱]. این گزارش پایه و اساس شناسایی رفتار های ناهنجار در سیستم های کامپیوتری محسوب می شود. این مدل به خودی خود تهدیدات را به سه گروه: نفوذ های خارجی، نفوذ های داخلی و خطا تقسیم بندی می کند. در سال ۱۹۸۷، یک مدلی برای سیستم های تخصصی تشخیص نفوذ آنی با هدف شناسایی و تشخیص طیف وسیعی از مسائل امنیتی متغیر، از ورود غیرمجاز و حک کردن توسط مهاجمان و سوءاستفاده توسط گروه های کاربران ایجاد شد[۲]. این مدل براساس این ایده است که نفوذ امنیتی به هر سیستم را بتوان شناسایی و با تحلیل سیستم، پایش کرد. این مدل به نوبه خود یک چارچوب برای سیستم های تخصصی تشخیص نفوذ با اهداف عمومی است که هنوز در مطالعات امروزه نیز از آنها استفاده می شود[۳]. دو روش اصلی مورد استفاده در سیستم های تشخیص و پیشگیری از نفوذ، تلفیق شده و تشکیل سیستم تشخیص نفوذ هوشمند(CIIDS) [۴] را می دهند. با مطالعه به بررسی و حل برخی چالش های فعلی برای سیستم های تشخیص نفوذ و الگوریتم های مورد استفاده برای همبستگی هشدار پرداخته و در یک رویکرد ساختارمند به سیستم های تشخیص نفوذ با تعریف و طبقه بندی اجزای سیستم(IDS) تشریح می شود. این طبقه بندی یک درک واضح از همه بخش های تشکیل دهنده سیستم های تشخیص نفوذ و چالش هایی را که سیستم با آنها رو بروست در اختیار می گذارد. جیمز و جوی به بررسی شیوه ای در خصوص فنون و روش های مورد استفاده در تشخیص نفوذ پرداختند[۶]. بررسی فنی سیستم های تشخیص نفوذ با بررسی اصول چگونگی ساخت سیستم ها و روش هایی که آنها برای شناسایی و تشخیص تهدیدهای امنیتی بالقوه استفاده می کنند آغاز می شود[۷]. همچنین این مقاله توضیح می دهد که چگونه یک سیستم تشخیص نفوذ می تواند به نقض سیاست های امنیتی ای که آنها پایش می کنند پاسخ دهد. سیستم های تشخیص و پیشگیری از نفوذ دارای مسائل مختلف مقیاس پذیری و کارایی است[۸]. این روش به سیستم های تشخیص و پیشگیری از نفوذ امکان می دهد تا دارای سرعت و دقت بالایی باشند. روش های تشخیص ناهنجاری همگی با یک سری مسائل مربوط به مثبت های کاذب مواجه اند و یک سیستم تشخیص جدید برای روش های مبتنی بر ناهنجاری وجود دارد که تعادل بین بسیاری از تعمیمات را برهم می زند[۹]. ترکیب این دو روش، از مناسب ترین شیوه ها در الگوریتم ها و سیستم های تشخیص و پیشگیری از نفوذ محسوب می شود که به نوبه خود از هر دو روش مبتنی بر ناهنجاری و تطبیق الگو برای دستیابی به سیستم تشخیص بهتر بهره می برد[۱۰]. در پیشنهادی برای یک سیستم تشخیص و پیشگیری از نفوذ مبتنی بر امضاء[۱۱]، محققان به ارایه تفاسیر سازماندهی پایه از سیستم های تشخیص و پیشگیری از نفوذ پرداخته اند.

۳. روش های IDPS

روشهای بسیاری توسط IDPS برای تشخیص تغییرات در سیستم هایی که پایش می کنند مورد استفاده قرار می گیرند. این تغییرات می توانند شامل تهاجمات خارجی و یا سوءاستفاده توسط یک پرسنل و کاربر داخلی باشند. در میان روش های بسیار، چهار روش برجسته تر بوده و استفاده فراوانی دارند. چهار سیستم و روش تشخیص مورد استفاده توسط سیستم های تشخیص و پیشگیری از نفوذ(IDPS)، شامل: مبتنی بر امضاء یا تطبیق الگو، مبتنی بر ناهنجاری، مبتنی بر تجزیه و تحلیل الگوی چند

تراکنشی و مبتنی بر هیبرید می باشند. جدید ترین سیستم های IDPS از روش های هیبرید استفاده می کنند، که ترکیبی از دیگر روش ها با قابلیت های تشخیص و پیشگیری از نفوذ بهتر می باشند. این روش ها از یک مدل یکسان عمومی و کلی استفاده کرده و تفاوت های میان آنها در نحوه پردازش اطلاعاتی است که آنها از محیط های پایش شده، برای تعیین تهاجمات و یا تخطی ها جمع آوری کرده اند. شکل۱ ساختار کلی را می دهد که سیستم ها بر مبنای آن سازمان دهی می شوند. این ساختار توسط گروه محققین تشخیص نفوذ ایجاد شده و دارای چهار بلوک کارکردی و عملیاتی است که بلوک های وقایع در برگیرنده باکس های یکنواختی می باشند که رویدادها را از سیستم پایش جمع آوری کرده و توسط بلوک های دیگر تجزیه و تحلیل می شوند و سپس بلوک های دیتابیس که باکس های دیتابیس هستند که رویدادها و وقایع را از بلوک های وقایع ذخیره می کنند و یک پیام هشدار ارسال می کنند و در نهایت بلوک های پاسخ وجود دارد که هدف آن واکنش به یک نفوذ و یا توقف آن است [۱۲].



شکل ۱- ساختار کلی سیستم IDPS

۱.۳. روش مبتنی بر ناهنجاری

سیستم کار روش مبتنی بر ناهنجاری مقایسه فعالیت مشاهده شده در برابر یک پروفیل معیار است. پروفیل معیار یک رفتار نرمال آموزش دیده شده از سیستم پایش است و طی دوره یادگیری توسعه داده می شود و IDPS محیط را یادگرفته و ایجاد یک پروفیل نرمال از سیستم پایشی می کند. این محیط می تواند شامل شبکه ها، کاربران، سیستم ها و غیره باشد.

این پروفیل ممکن است ثابت و یا پویا باشد. یک پروفیل ثابت، با تثبیت شدن دیگر تغییر نمی کند، در حالی که یک پروفیل پویا با پایش و تکامل سیستم تغییر می کند [۱۳]. یک پروفیل پویا یک سری داده های اضافی را به IDPS برای بروزرسانی پروفیل می افزاید که آن را باز و به درون آن نفوذ می کند. یک مهاجم می تواند به IDPS هایی حمله کند که از پروفیل پویا با پخش حمله و در دوره زمانی طولانی حمله می کند. در حین حمله او، تهاجم او بخشی از پروفیل با نفوذ IDPS و تغییرات آن درون پروفیل به عنوان تغییرات طبیعی نامگذاری می شود. با استفاده از آستانه از پیش تعیین شده هرگونه انحرافات خارج از آستانه به عنوان تهاجم مطرح می شود. یک پروفیل ثابت در شناسایی حملات و تهاجم های جدید بسیار کارآمد است زیرا هرگونه تغییر از رفتار نرمال به صورت ناهنجاری طبقه بندی می شود.

در ساختار نامتمرکز خلاف روش قبلی کنترل مرکزی وجود ندارد بلکه بات‌ها به صورت یک شبکه نظیر به نظیر با هم در تعامل می‌باشند. سرکرده دستورات خود را به یک یا چند بات ارسال می‌کند و با استفاده از قراردادهای نظیر به نظیر این دستورات در تمام بات‌نت منتشر می‌شود. حسن این روش این است که تمام بات‌ها به کارساز فرمان-کنترل وابسته نیستند. توزیع ترافیک در این بات‌نت‌ها شناسایی آنها را دشوار کرده است. این بات‌نت‌ها مقیاس‌پذیری بالایی دارند اما پیاده‌سازی آنها پیچیده و دشوار است. بات‌ها به خاطر تاخیر در انتشار دستورات نمی‌توانند به سرعت آرایش بگیرند. حالت خاصی هم از بات‌نت‌های نظیر به نظیر موجود است که در آن هر بات فقط با یک بات دیگر در ارتباط است. در نتیجه گراف اتصال حاصل

از این شبکه به صورت زنجیر است. این پیاده‌سازی گرچه از مدل کامل نظیر به نظیر ساده‌تر است ولی تاخیر انتشار در آن زیاد است و تضمینی نیز برای رسیدن پیام به همه بات‌ها وجود ندارد، زیرا این روش از این ضعف رنج می‌برد که در صورت قطع شدن زنجیر بخشی از بات‌نت از دسترس خارج می‌گردد، در نتیجه چنین ساختاری از استحکام مطلوبی برخوردار نیست. به طورکلی روش‌های شناسایی ترافیک‌های مختلف شبکه از زمره چالش‌های باز در حوزه کنترل ترافیک است [۴]. فراهم‌کنندگان سرویس‌های اینترنت (ISP) از منظر استفاده بهینه از پهنای باند، بسیار مشتاقند که ابزاری در اختیار داشته باشند که بتوانند انواع ترافیک موجود در شبکه خود را شناسایی کنند و اجازه عبور ترافیک‌های ناخواسته را ندهند. متخصصان امنیت شبکه نیز به دنبال شناسایی ترافیک‌های خطرناک مثلاً ترافیک ناشی از فعالیت یک نفوذگر یا انتشار یک کرم می‌باشند. اما همانگونه که گفته شد، این حوزه هنوز به بلوغ کافی نرسیده است. ترافیک ناشی از فعالیت یک بات‌نت هم به عنوان بخشی از ترافیک شبکه است. علاوه برآن، ترافیک ناشی از یک بات‌نت بسیار شبیه ترافیک نرمال است و همین امر شناسایی آنرا دشوارتر کرده است. روش‌های گوناگونی برای شناسایی بات‌نت‌ها ارایه شده‌اند ولی هنوز جامعیت لازم را ندارند و میزان خطایشان بالاست. در ادامه به بررسی اجمالی چند روش شناسایی بات‌نت‌ها می‌پردازیم و درپایان هم یک دسته‌بندی از روش‌های شناسایی بات‌نت ارایه خواهد شد.

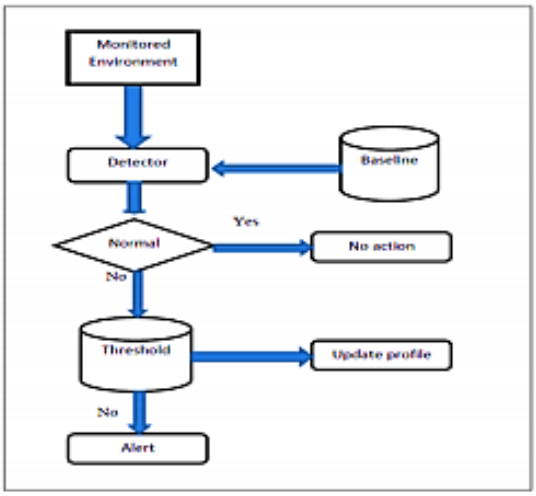
روشهای مبتنی بر ناهنجاری می توانند تهاجمات روز صفر را در محیط بدون به روز سازی سیستم شناسایی کنند. روش تشخیص نفوذ مبتنی بر ناهنجاری از سه شیوه عمومی برای شناسایی و تشخیص ناهنجاری ها استفاده کرده و این شیوه ها شامل تشخیص ناهنجاری آماری، داده و دانش کاوی و روش مبتنی بر یادگیری ماشینی می باشند [۱۳]. در این روش، یک نما از رفتار عادی ایجاد می‌شود. یک ناهنجاری ممکن است نشان دهنده یک نفوذ باشد. برای ایجاد نماهای رفتار عادی از رویکردهایی از قبیل شبکه‌های عصبی، تکنیک‌های یادگیری ماشین و حتی سیستم‌های ایمنی زیستی استفاده می‌شود. برای تشخیص رفتار غیرعادی، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آن‌ها پیدا کرد. رفتارهایی که از این الگوها پیروی می‌کنند، عادی بوده و رویدادهایی که انحرافی بیش از حد معمول آماری از این الگوها دارند، به عنوان رفتار غیرعادی تشخیص داده می‌شود. نفوذهای غیرعادی برای تشخیص بسیار سخت هستند، چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد. معمولاً رویدادی که بسیار بیشتر یا کمتر از دو استاندارد انحراف از آمار عادی به وقوع می‌پیوندد، غیرعادی فرض می‌شود. به عنوان مثال اگر کاربری به جای یک یا دو بار ورود و خروج عادی به سیستم در طول روز، بیست بار این کار را انجام دهد، و یا رایانه‌ای که در ساعت ۲:۰۰ بامداد مورد استفاده قرار گرفته در حالی که قرار نبوده کامپیوتر فوق پس از ساعت اداری روشن باشد. هر یک از این موارد می‌تواند به عنوان یک رفتار غیر عادی در نظر گرفته شود.

فنون ناهنجاری آماری برای ساختن دو پروفیل مورد نیاز یکی طی مرحله یادگیری که به عنوان پروفیل معیار مورد استفاده قرار می گیرد و پروفیل فعلی که با پروفیل معیار مقایسه می شود و بیانگر هرگونه تفاوت به صورت ناهنجاری ها است که بستگی به شرایط آستانه محیط پایش شده دارد [۱۴] مورد استفاده قرار می گیرند. آستانه ها باید بر اساس نیازمندی ها و رفتار محیط مورد پایش برای عملکرد هر چه کارآمدتر سیستم تنظیم شوند.

روش مبتنی بر داده و دانش کاوی برای اتوماسیون، شیوه جست و جوی پایش ها برای ناهنجاری ها استفاده شده و این اهمیت بسیار زیادی در مرحله پردازش داده ها دارد. این روش بیشترین تعداد مثبت های کاذب و منفی های کاذب را به دلیل وجود داده های بالادست در اختیار می گذارد که ناشی از وظیفه پیچیده شناسایی و تصحیح مقوله بندی رویدادهای مشاهده شده در سیستم است [۱۵]. روش یادگیری ماشینی به تجزیه و تحلیل درخواست های سیستم پرداخته و یک روشی است که استفاده و کاربرد فراوانی دارد [۱۶].

ساختار کلی سیستم IDPS مبتنی بر ناهنجاری در شکل ۲ نشان داده شده است. محیط پایش شده توسط شناساگر پایش می شود که به بررسی وقایع مشاهده شده در برابر پروفیل معیار می پردازد. اگر رویدادهای مشاهده شده مطابق با معیار باشد،

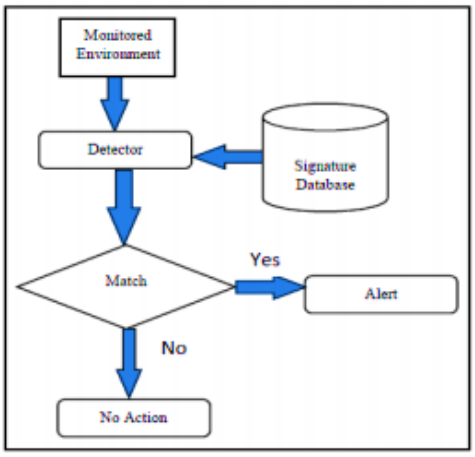
هیچگونه اقدامی نمی شود، اما اگر مطابق با پروفیل معیار نباشد و در آستانه قابل قبول باشد آنگاه پروفیل بروزرسانی می شود. اگر رویدادهای مشاهده شده مطابق با پروفیل معیار نباشد و خارج از محدوده و آستانه مورد نظر باشد، آنگاه می توان آنها را به عنوان ناهنجاری نامیده و فرمان خطر و یا هشدار صادر می شود.



شکل ۲- ساختار روش شناسی مبتنی بر ناهنجاری

۲.۳. روش مبتنی بر امضاء

ساختار کلی روش مبتنی بر امضاء و یا تطبیق الگو در شکل ۳ نشان داده شده است. این ساختار از شناساگر برای یافتن و مقایسه امضاءهای فعالیت موجود در محیط پایش شده و امضاءهای شناخته شده در دیتابیس های امضاء استفاده می کند. اگر تطبیق صورت گرفت، یک فرمان هشدار صادر شده و در غیر این صورت، شناساگر اقدامی نمی کند.



شکل ۳- ساختار روش شناسی مبتنی بر امضاء

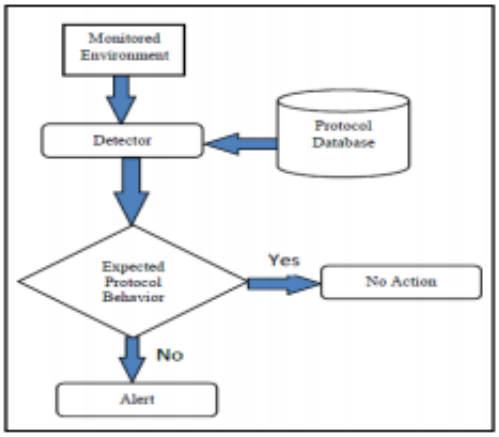
روش مبتنی بر امضاء به مقایسه امضاءها و الگوهای مشاهده شده با الگوها و امضاءهای روی فایل می پردازد. این فایل می تواند یک دیتابیس و یا لیستی از امضاءهای تهاجمی شناخته شده باشد. در این تکنیک که معمولاً با نام تشخیص مبتنی بر امضاء شناخته شده‌است، الگوهای نفوذ از پیش ساخته شده (امضاء) به صورت قانون نگهداری می‌شوند. به طوری که 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 تشخیص دهنده دارای پایگاه داده‌ای از امضاءها یا الگوهای حمله است و سعی می‌کند با بررسی ترافیک شبکه، الگوهای مشابه با آنچه را که در پایگاه داده خود نگهداری می‌کند، بیابد. این دسته از روش‌ها تنها قادر به تشخیص نفوذهای شناخته شده می‌باشند و در صورت بروز حملات جدید در سطح شبکه، نمی‌توانند آن‌ها را شناسایی کنند و مدیر

شبکه باید همواره الگوی حملات جدید را به سامانه تشخیص نفوذ اضافه کند. از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آن‌ها عیناً به سیستم داده شده‌است. هرگونه امضای مشاهده شده در محیط پایش شده که مطابق با امضای روی فایل نباشد، به صورت تجاوز به سیاست امنیتی و یا تهاجم تلقی می شود. IDPS امضاء محور دارای خطای زیادی است، زیرا هرگونه فعالیت و ترافیک شبکه را در محیط پایش شده بررسی نمی کند. در عوض تنها به جست و جوی امضاءها و الگوهای شناخته شده در دیتابیس یا فایل می پردازد. بر خلاف روش مبتنی بر ناهنجاری، سیستم روش مبتنی بر امضاء را به آسانی می توان مورد استفاده قرار داد زیرا نیازی به یادگیری محیط ندارد [۱۶]. وظیفه این روش جست و جو، بازرسی و مقایسه محتویات بسته های شبکه ای از نظر وجود علایم یا امضاءهای تهدید کننده است. همچنین این روش به مقایسه امضاءهای رفتاری در برابر امضاءهای رفتاری مجاز می پردازد. روش مبتنی بر امضاء به تجزیه و تحلیل درخواست های سیستم های شناختن تهدیدهای قریب الوقوع می پردازد [۱۷]. همچنین روش مبتنی بر امضاء در برابر تهاجمات و حملات شناخته شده بسیار کارآمد عمل می کند، اما نمی تواند حملات جدید را شناسایی کند، مگر اینکه با امضاءهای جدید به روز شود. روش های تشخیص و پیشگیری مبتنی بر امضاء به آسانی مورد تهاجم قرار می گیرند، زیرا بر اساس روشها و حملات شناخته شده بوده و بستگی به امضاهای جدید قبل از شناسایی تهاجمات دقیق دارند [۱۸]. سیستم های تشخیص مبتنی بر امضاء به آسانی توسط مهاجمانی حک می شوند که حملات شناخته شده و سیستم های هدفی را که با امضاءهای جدید بروز نشده و قادر به شناسایی تغییرات نیستند، تغییر می دهند. روشهای مبتنی بر امضاء مستلزم در اختیار داشتن منابع مهمی با تعداد بی نهایت از تغییرات در تهدیدات شناخته شده است. روش مبتنی بر امضاء را به آسانی می توان تغییر و بهبود بخشید، زیرا عملکرد آن براساس امضاءها و نقش های به کار گرفته شده است [۱۹].

۳.۳. روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی

عملکرد روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی، براساس مقایسه پروفیل های تثبیت شده و در خصوص چگونگی رفتار پروفیل ها در برابر رفتار مشاهده شده است. پروفیل های پروتکل تثبیت شده توسط فروشندگان طراحی و تثبیت می شوند. برخلاف روش مبتنی بر تطبیق الگو و یا امضاء، که تنها به مقایسه رفتار مشاهده شده در برابر یک لیست می پردازد، روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی دارای دانش و درک عمیقی از چگونکی کارکرد و اثرات متقابل بین پروتکل ها و نرم افزارهاست. این دانش و تجزیه و تحلیل عمیق تاثیر بسزایی را در عملکرد و کارایی سیستم دارد [۱۳]. روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی، دیگر روشهای تشخیص و پیشگیری از نفوذ را به خوبی با هم تلفیق کرده و ایجاد روش های هیبرید و یا ترکیبی می کند [۱۹]. دانش و درک عمیق روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی در خصوص چگونکی رفتار پروتکل به عنوان پایه و اساس ایجاد روشهای تشخیص و پیشگیری از نفوذ است که رفتار ترافیک وب را درک کرده و برای حفاظت از وب سایت ها کارآمد و موثر می باشند [۱۹]. اگرچه روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی دارای دانش عمیقی از پروتکل های پایش شده است، اما به آسانی در معرض تهاجماتی قرار می گیرد که در چارچوب رفتار قابل قبول پروتکل ها باقی می مانند. روش ها و فنون مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی کمتر مورد استفاده قرار گرفته و با روش های دیگر طی دهه های گذشته تلفیق و ترکیب شده اند. این خود منجر به کاهش و تنزل عملکرد سیستم های تشخیص و پیشگیری از نفوذ شده است که تنها از روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی بهره می برد. عمده مطالعات و تحقیقات انجام شده بر روی روش های سیستم های تشخیص و پیشگیری از نفوذ، بر روش های ناهنجاری، امضاء و هیبرید متکی بوده اند که موجب کاهش بیشتر تغییرات روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی به عنوان یک روش پیشرو IDPS گردیده است.

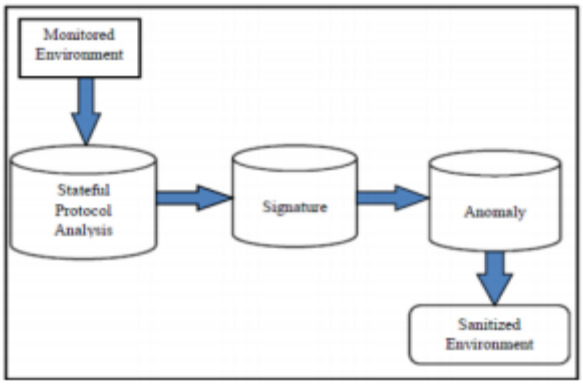
ساختار کلی روش مبتنی بر تجزیه و تحلیل پروتکل چند تراکنشی در شکل ۴ نشان داده شده است. این ساختار مشابه با ساختار روش مبتنی بر امضاء با یک استثناء می باشد که به جای دیتابیس امضاء، روش مبتنی بر تجزیه و تحلیل پروتوکل چند تراکنشی از رفتار پروتکل قابل قبول در آن دیده می شود.



شکل ۴- روش مبتنی بر تجزیه تحلیل پروتوکل چند تراکنشی

۴.۳. روش مبتنی بر هیبرید

روش مبتنی بر هیبرید به مقایسه دو یا چند مورد از روش های دیگر می پردازد. نتیجه اصلی، روش بهتری است که از نقاط قوت روش های ترکیبی بهره می برد. نخستین روش هیبرید IDS است که یک قالب کاری بر اساس فرمت تبادل پیام تشخیص نفوذ (IDMEF) از یک استانداردIETF بوده و امکان برقراری ارتباط را به سنسور های مختلف می دهد [۲۰]. در Snort [۲۱] با افزودن یک موتور مبتنی بر ناهنجاری به موتور مبتنی بر امضاء برای ایجاد تشخیص بهتر اصلاح شده و سپس سیستم های هیبریدی جدید در برابر Snort منظم با همین داده های آزمایشی تست می شود. سیستم هیبرید نفوذهای بیشتری را نسبت به یک سیستم منفرد شناسایی و تشخیص می دهد. یک سیستم تشخیص نفوذ هیبرید از شبکه های سنسور بی سیم خوشه محور پیشنهاد شدند، که هدف آنها حک کردن سیستم هایی بود که از مدل مبتنی بر ناهنجاری برای فیلتر داده ها و مدل مبتنی بر امضاء برای شناسایی نفوذ بهره می برد. دیگر مدل برای روش هیبرید بر اساس چگونگی کارکرد سیستم ایمنی بدن انسان پیشنهاد شد [۲۲]. سیستم پیشنهادی بر اساس قالب کاری از سیستم ایمنی بدن انسان است که از ساختار هیبریدی استفاده می کند که هر دو رویکرد تشخیص ناهنجاری و سوءاستفاده را به کار می برد [۲۲]. شکل کلی این روش مبتنی بر هیبرید در شکل ۵ نشان داده شده است، ۵ روش دیگر با هم ترکیب شده اند. محیط پایش شده توسط روش نخست تجزیه و تحلیل شده و سپس به دیگری انتقال داده می شود و در نهایت به آخری می رسد. این ایجاد سیستم بهتری می کند.



شکل ۵- ساختار روش مبتنی بر هیبرید

۴. ارزیابی روش ها

این بخش به توصیف ارزیابی روش های تشخیص و سیستم های پیشگیری نفوذ (IDPS) و سیستم هایی که بر اساس این روشها می باشند می پردازد. جدول۱ به ارزیابی انواع روشهای تشخیص و سیستم های پیشگیری نفوذ (IDPS) می پردازد که آیا آنها از هر سه روش اصلی استفاده می کنند و یا اینکه ترکیبی از دو یا چند روش دیگر است.

جدول ۱- پارامتر های ارزیابی روش های IDPS

شاخص ارزیابی	ناهنجاری	امضاء	آنالیز پروتکل چند تراکنشی	هیبرید
مقاومت در برابر تهاجم	متوسط	پایین	پایین	بالا
صحت بالا	متوسط	متوسط	متوسط	بالا
سهم بازاری	متوسط	بالا	متوسط	متوسط
توسعه پذیری	بالا	بالا	بالا	متوسط
سطح بلوغ	متوسط	بالا	بالا	بالا
خطا در سیستم پایش شده	پایین	پایین	پایین	متوسط
نگهداری	پایین	متوسط	متوسط	متوسط
عملکرد	متوسط	بالا	بالا	متوسط
سهولت ترکیب	خیر	بله	بله	بله
سهولت استفاده	بالا	پایین	پایین	پایین
حفاظت در برابر حملات جدید	بالا	پایین	متوسط	بالا
مثبت های کاذب	بالا	پایین	پایین	پایین
منفی های کاذب	بالا	متوسط	متوسط	پایین

۵. برخی راهکارها برای برقراری یک سیستم امن پیشگیری از نفوذ (IPS)

یک سیستم پیشگیری از نفوذ شامل تمام مواردی است که می تواند یک مخرب را شناسایی کند، در ضمن توانایی شناسایی ترافیک مخرب نیز از وظایف آن است. وقتی که این سیستم فعال باشد، بطور معمول می توان با جلوگیری از دسترسی عامل نفوذگر به هدف و برقراری ارتباط، حمله ها را بی اثر ساخت.

۱.۵. سیستم پیشگیری و تشخیص نفوذ(IDPS) به صورت همزمان

IPS می تواند دقیقاً بر اساس نیاز تنظیم شود. در حالت شناسایی IDS سیستم ترافیک را مانند یک ناظر کنترل و بازبینی می کند. در حالت جلوگیری IPS دستگاه در مسیر ترافیک قرار دارد. هم IPS و هم IDS بهتر است که بتوانند پکت های مخرب شناسایی شده را با ساخت لیست سیاه (Black list) به فایروال گزارش داده و یا مستقلاً دسترسی آنها را بلاک کنند. یک IPS اگر دقیقاً از وجود یک مورد نفوذی و مخرب آگاه شود مستقلاً می تواند اقدام به پاکسازی مسیر نماید. در حالت

همزمان هر دو سیستم IPS و IDS برای شناسایی و جلوگیری استفاده شده و عملکرد بهینه آنها حتی از نظر اقتصادی نیز به صرفه است.

۲.۵. حفاظت AET تکنیک های پیشرفته گریز (Advanced Evasion Techniques)

AET ها در حال حاضر در آزمایشگاه های NSS برای آزمایش محصولات امنیتی استفاده می شوند. بررسی AETها نیازمند بازرسی دقیق جریان اطلاعات است که ۹۵٪ از سازمان ها این کار را انجام نمی دهند. بسیاری از دستگاه های امنیتی در حال حاضر بصورت مجزا AET را بررسی نمی کنند و در بهترین حالت گزارش موارد مشکوک یا مشکل دار اعلام می شود.
بسیار مهم است که روش ها با راه کار ها اشتباه نشوند. استاکس نت در زمانی شناسایی می شد که هدف را مورد حمله قرار داده بود، در حالی که در آنجا حضور داشت و امکان شناسایی کد آن بعد از یکبار شناسایی، کار سختی نیست. اگر IPS کلیه ترافیک را ذخیره کند AET ها می توانند مورد آنالیز و بررسی قرار گیرند.

۳.۵. ارتباط با رویدادها Event Corelation

ارتباط با رویدادها می تواند تعداد خطاهای کاذب را کاهش داده و سرویس حفاظتی دقیق تری ارائه کند. این سیستم بصورت لحظه ای با نگاه به چند منبع ثبت رویداد بدنبال رویدادهای مخرب می گردد. سیستم فشرده سازی رویدادها، رویدادهای تکراری را حذف کرده و حداقل منابع را مصرف می کند که خصوصاً برای ارتباط های راه دور با دفتر مرکزی می تواند بسیار سودمند باشد. یک سیستم Event Corelation خوب با IPS ارتباط برقرار کرده و یک حمله یا یک Worm را کاملاً ایزوله کرده و با ارتباط با فایروال و IPS بصورت همزمان آسیب را به حداقل می رساند.

۴.۵. فیلتر مسیرهای وب (Web filtering)

فیلتر محتوای وب یک ابزار بسیار سودمند برای IPS شماست که مزایای چندگانه ای نظیر جلوگیری از دسترسی به سایت های شناخته شده با محتوای مخرب یا تقلبی در کنار مدیریت پهنای باند با مدیریت دسترسی ها به سایتهایی که استفاده از آنها مورد نیاز سازمان نیست بسیار مفید خواهد بود. سیستم های پیشرفته web filtering راهکار های متنوعی را در اختیار شما خواهند گذاشت، مانند لیست های سیاه یا سفید (Whitelist & Blacklist) که به کمک آنها می توانید قوانین دسترسی به کل شبکه را مدیریت کنید. در عین حال می توانید گزارش هایی را بر اساس رفتار های استفاده از وب و سایت های مورد درخواست آماده کنید.

۵.۵. دسترسی امن و بازرسی (Secure socket layer Inspection)

تکنولوژی بازرسی SSL بسیار حیاتی است، زیرا به کمک آن می توانیم مطمئن شویم که هیچ حمله ای با جا زدن خود در پکت های رمزنگاری Https، وارد یا خارج نشده است. این قابلیت به ادمین این توانایی را خواهد داد که ترافیک کدگذاری شده را بازرسی کرده و در مقابل عوامل مضر عکس العمل نشان دهد. IPS شما باید دارای راه کنترل شده ای برای باز کردن رمزها بصورت متن باشد(Clear Text) و بتواند این مشکل را برطرف کند و در عین حال این تکنولوژی برای برآوردن نیازهای PCI DSS (استانداردی در ارتباط با کارت های پرداخت الکترونیک) نیز ضروری است.

۶.۵. حفاظت در برابر حمله های DOS (Denial Of Service)

IPS شما باید بتواند در برابر ورود ترافیک های غیرضروری و جریان های DOS ، بدون ایجاد مشکل برای ترافیک عادی حفاظت شود. روشهای حمله Connection flood یا Web service starvation برای خارج از سرویس ساختن یک

سرور یا سرویس دهنده مواردی از اینگونه حمله هستند. حمله های سیل TCP SYN می توانند با جلوگیری از تکرار درخواست ها از طرف آدرس های جعلی و جلو گیری از اتصال آدرس های جعلی به منابع بلاک و دفع شوند. IPS شما باید به سرعت مراکز اصلی اتصال های جعلی را شناخته و دسترسی آنها را ببندد، در حالیکه اتصال ها و کاربران عادی خللی در کارشان ایجاد نگردد. حمله های UDP flood را نیز می توان با محدود نمودن پکت های دریافتی بر اساس الگو های استاندارد به وب سرور کنترل کرد. با استفاده از تکنیک های ارتباطی در شناسایی الگوهای رفتارهای مخرب در برابر اتصال به سرویس دهنده های وب، وقتی یک سیستم درخواست اتوماتیکBotnet شناسایی شود IPS دسترسی و ارتباط آنرا محدود و قطع می نماید.

۷.۵. امکان مدیریت مرکزی

مدیریت مرکزی برای یک سیستم IPS بسیار حیاتی است، زیرا که به شما این امکان را خواهد داد تا هر دستگاه را بدون اینکه لازم باشد بصورت فیزیکی دسترسی داشته باشید، تنظیم کرده و تغییرات لازم را اعمال نمایید. مدیریت مرکزی عموماً به شما این قابلیت را خواهد داد که دستگاهای IPS و امکانات آنرا مدیریت و کنترل نمایید، اخطارها را رسیدگی کرده ، عملیات ارتقا را مدیریت کنید ، و فایروال و تنظیمات IPS را بروز نمایید. در عین حال با مدیریت متمرکز در زمان کوتاه تری می توان، در شرایط خاص امنیتی راه کار های لازم را انتخاب و اعمال کرد.

۸.۵. کارایی

IPS شما اگر به صورت صحیح تنظیم و راه اندازی نشده باشد، یا مناسب نباشد، می تواند کارایی کاهش یابد.به قابلیت بخش بندی Clustering برای به اشتراک گذاشتن کانکشن های ارتباطی نگاه کنید که می تواند کارایی را افزایش داده و downtime را کاهش دهد. راه اندازی صحیح بخش های مختلف IPS می تواند کاهش کارایی و سرعت را به حداقل برساند. IPS می تواند ترافیک را ذخیره و بررسی کند، سپس با جدا سازی بخش های مختلف و آنالیز آن توسط سیستم های جداگانه می توان کارایی را افزایش داد. برای بهترین تنظیمات بهتر است از تولید کننده IPS خود، راهکارهای مناسب برای بهترین روش راه اندازی را درخواست کنید.

۹.۵. آمادگی برای IPv6

سیستم عامل های اصلی و همچنین تولید کنندگان اصلی تجهیزات شبکه همگی از IPv6 پشتیبانی می کنند. برای مثال سیستم عامل ویندوز از نسخه ویستا بصورت پیش فرض از IPv6 پشتیبانی می کند که در این حالت اگر راهکارهای امنیتی لازم در نظر گرفته نشود می تواند یک تهدید امنیتی به حساب آید. در عین حال برخی از ترافیک های مخرب می تواند در IPv6 بصورت مخفی حرکت کرده و تونل های IP-IP نیز می توانند منبع مشکلات امنیتی فراوانی باشند، باید مطمئن شد که IPS شما بررسی های عمیق بر روی ترافیک پکت های IPv6، IP-in-IP، GRE Tunneling را پشتیبانی کرده و رهگیری لازم نیز انجام می گیرد (statefull and deep packet inspection)

۱۰.۵. هماهنگی و یکپارچگی کامل با فایر وال

کارایی واقعی نسل جدید فایروال ها زمانی کامل است که بتواند کارایی هایش را با یک سیستم مجتمع تشخیص و پیشگیری از نفوذ (IDPS) هماهنگ و یکپارچه کند و این مهم می تواند در یک دستگاه بصورت مجتمع یا جداگانه باشد. و لی دقت در کارایی، سرعت و مدیریت (management&Throughput) این مجموعه حرف اول را خواهد زد.

۶. روش پیشنهادی جهت تحلیل

استفاده از شبکهٔ عصبی در قسمت تحلیل که باعث اجتناب از تولید صریح قوانین تشخیص می شود، همچنین قابلیت شبکهٔ عصبی در تشخیص حمله های شناخته شدهٔ تغییر شکل یافته و قابلیت ادارهٔ داده های نویزی و ناقص و مصرف کم منابع سیستم از دیگر مزیت های آن به شمار می رود. با استفاده از شبکهٔ عصبی، دیگر نیازی به استخراج خصوصیات مشترک هر دسته از این رفتارها نیست، چرا که شبکهٔ عصبی، خود می داند که چگونه در حین آموزش ویژگی های مشترک هر دسته از رفتارها را استخراج و در خود ثبت نماید.

۷. نتیجه‌گیری

این مقاله چهار روش اصلی مورد استفاده در سیستم های تشخیص و پیشگیری از نفوذ،۱۰راهکار امن سازی و یک پیشنهاد جهت تحلیل سیستم ارایه داد. چهار سیستم و روش تشخیص مورد استفاده توسط سیستم های تشخیص و پیشگیری از نفوذ(IDPS)، شامل: مبتنی بر امضاء یا تطبیق الگو، مبتنی بر ناهنجاری، مبتنی بر تجزیه و تحلیل الگوی چند تراکنشی و مبتنی بر هیبرید می باشند، اگرچه روش مبتنی بر ناهنجاری نسبت به سه روش دیگر در شناسایی تهدیدات بدون بروزرسانی و یا ورودی برای کاربر ها مزیت بیشتری دارد اما بیشتر سیستم های تشخیص و پیشگیری از نفوذ امروزی از ترکیبی از چهار روش بهره می برند. این مقاله شیوه های مقایسه و ارزیابی آسان روش های سیستم های تشخیص و پیشگیری از نفوذ مورد استفاده در بازار را ارایه نمود. ۱۰ راهکار عملی جهت ایجاد یک سیستم امن برای تشخیص و جلوگیری از نفوذ و همچنین روشی مفید و دقیق جهت تحلیل سیستم را ارائه داد.

۸. منابع

1. Animesh Patcha, Jung-Min Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends, Computer Networks,” The International Journal of Computer and Telecommunications Networking, Vol.51, No.12, August, 2007, pp.3448-3470.
2. Rebecca Bace, “An introduction to intrusion detection and assessment for system and network security management.” ICSA Intrusion Detection Systems Consortium Technical Report, 1999.
3. James P. Anderson, “Computer security threat monitoring and surveillance,” James P. Anderson Co., Fort Washington, Pennsylvania, technical Report, April 1980.
4. Tarek S. Sobh, “Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art,” Computer Standards & Interfaces 28 , 2006, pp. 670– 694.
5. Fredrik.Valeur, Giovanni Vigna, Christopher Kruegel, Richard A. Kemmerer, “A comprehensive approach to intrusion detection alert correlation,” IEEE Transactions on Dependable and Secure Computing, Vol. 1, NO. 3, 2004.
6. Shelly X. Wu, Wolfgang Banzhaf, “The use of computational intelligence in intrusion detection systems: A review,” Applied Soft Computing Journal 10, 2010, pp. 1-35.
7. Xuan D. Hoang, Jiankun Hu, Peter Bertok, “A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference,” Journal of Net- work and Computer Applications 32, 2009, pp. 1219–1228.
8. Elshoush H. Tagelsir, Izzeldin M. Osman, “Alert correlation in collaborative intelligent intrusion detection systems—A survey.” Applied Soft Computing 11, 2011, pp. 4349-4365.
9. Shanbhag, Shashank, Tilman Wolf. “Accurate anomaly detection through parallelism.” IEEE Network 23.1, 2009, pp. 22-28.
10. James Cannady, Jay Harrell, “A comparative analysis of current Intrusion detection technologies,” Houston 1996, Proc. 4th Technology for Information Security Conference.

11. Bejtlich, Richard, “The Tao of Network Security Monitoring: Beyond Intrusion Detection,” Addison-Wesley, 2004.

12. Terry Brugger, “KDD cup’99 dataset (network intrusion) considered harmful,” http://www.kdnuggets.com/news/2007/n18/4i.html, 2007.

13. Karen Scarfone and Peter Mell, “Guide to Intrusion Detection and PreventionSystems(IDPS),”

http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, 2007.

14. Pedro Garcı´a-Teodoroa, Jesus E. Dı´az-Verdejoa, Gabriel .Macia-Ferna´ndeza, Enrique Va´zquezb, “Anomaly-based network intrusion detection: Techniques, systems and challenge,” Computers Security 28.1-2, 2009, pp. 18-28.

15. Chih-Fong Tsai, YuFeng Hsu, Chia-Ying Lin, W.Y.Lin, “Intrusion detection by machine learning: A review,” Expert Systems with Applications, Vol 36, No.10. December 2009, pp.11994-12000.

16. Dorothy, Denning. “An intrusion-detection model,” IEEE Transactions on Software Engineering, Vol. SE-13, No.2. February, 1987.

17. Alfonso Valdes, Keith Skinner, “Probabilistic alert correlation,” 4th International Symposium on Recent Advances in Intrusion Detection (RAID2001), 2001, pp.54–68.

18. Indraneel Mukhopadhyay, Mohuya Chakraborty and Satyajit Chakrabarti, "A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems," Journal of Information Security, Vol. 2 No. 1, pp. 28-38.

19. Justin Lee, Stuart Moskovics, Lucas Silacci, “A Survey of Intrusion Detection Analysis Methods,” CSE 221, University of California, San Diego, Spring 1999.

20. Ning Weng, Luke Vespa, Benfano Soewito, “Deep packet pre-filtering and finite state encoding for adaptive intrusion detection system,” Computer Networks, Vol. 55, 2011, pp. 1648–1661.

21. Ali M. Aydın, Halim A. Zaim, Gokhan K. Ceylan, “A hybrid intrusion detection system design for computer network security,” Computers and Electrical Engineering, Vol. 35, 2009, pp. 517–526.

22. Kenneth L. Ingham, Anil Somayaji, “A Methodology for Designing Accurate Anomaly Detection Systems,” 4th international IFIPACM Latin American conference on Networking LANC 07, 2007, pp.139.