هشتمین همایش پژوهش های نوین در علوم و فناوری
زمستان ۱۳۹۵
Winter 2017
Conference on Recent Research in Science and Technology

افزایش قابلیتهای Snort برای هوشمند سازی سیستم تشخیص نفوذ

سید محسن هاشمی
دانشگاه آزاد اسلامی واحد بروجرد
ss_mohsen_hh@mailfa.com

چکیده

محرمانگی , تمامیت و در دسترس بودن , نگرانی های اصلی در توسعه و استخراج سیستم های یارانه ای مبتنی بر شبکه است . عظمت فراساختارهای شبکه ای , موجب افزایش آسیب پذیری این سیستم ها در قبال تهدیدهای امنیتی , حملات و نفوذ هاست .ارتباط شبکه های مختلف با یکدیگر و تنوع استفاده کنندگان سبب بروز مشکلات عمده ای نظیر سرقت , تخریب و دستکاری اطلاعات شده است . بدین منظور سیستم هایی تحت عنوان سیستم های تشخیص نفوذ به منظور شناسایی رفتارهای مشکوک به وجود آمده اند به طوریکه امروزه در شبکه های کامپیوتری از این سیستم ها به عنوان یک ابزار تدافعی در برابر حملات و به منظور حفاظت از اطلاعات استفاده میکنند.در این پایان نامه , رویکردی جدید نسبت به توسعه سیستم های تشخیص نفوذ هوشمند برای تشخیص حملات معرفی می شود . به این صورت که ضمن بررسی روش ها و تکنیک های تشخیص نفوذ و بررسی سیستم های تشخیص نفوذ , سیستم Snort را که به عنوان ابزاری مناسب , بخش وسیعی از امنیت شبکه ها را به خود اختصاص داده است را انتخاب و با ارائه روشی مناسب مهمترین محدودیت این سیستم که عدم تشخیص رفتار غیر عادی و حمله های جدید است را برطرف می نماییم . روش ارائه شده به میزان قابل توجهی درصد نرخ تشخیص را افزایش می دهد و تا ۲۰ درصد بهبود نسبت به وضعیت قبلی حاصل میشود .در این تحقیق از سیستم یادگیری $C_{4.5}$ استفاده می کنیم و پس از ایجاد قانون های جدید , این قوانین را برای هوشمند کردن Snort بکار می بریم .

کلمات کلیدی : Intrusion Detection, Snort , $C_{4.5}$ ، False Positive, False Negative

مقدمه

اطلاعات به عنوان یکی از مهمترین دارایی های سازمان ها تلقی میگردد.سازمان ها وابستگی خود را به اطلاعات بر اساس پردازش ها و استفاده روزمره از آن بسیار زیاد میدانند. استفاده بیش از پیش از تجارت الکترونیک باعث گردیده است تا مواردی نظیر حفظ امنیت اطلاعات نیز به میان بیاید.محرمانه بودن اطلاعات , یکپارچه بودن اطلاعات و حضور امن اطلاعات از بزرگترین نگرانی های موجود در عرصه شبکه های کامپیوتری هستند. سیستم تشخیص نفوذ توانایی کشف , جلوگیری و حتی واکنش بهحملات امنیتی را دارا میباشد.امروزه آن به عنوان عضو لاینفک امنیت اطلاعات در نظر گرفته می شود ولی اینمورد قابل ذکر است که از نظر فنی هیچ سیستمی وجود ندارد که بدون آسیب پذیری ایجاد گردد اینجاست که این سیستم تشخیص نفوذ می تواند موضوع خوبی برای تحقیق و توسعه باشد. بر اساس گزارشی اخیرا , تهدید سیستم های رایانه ای در پنج سال گذشته , ۲۵۰ درصد افزایش داشته است و منجر به ۱۰۰ بیلیون دلار خسارت گردیده است .از آنجا که همواره نفوذ و سواستفاده از سیستم ها و شبکه های کامپیوتری وجود دارد, و ساخت سیستم های خالی از اشکال , کاری بسیار مشکل و یا غیر ممکن می باشد , نیاز به در پیش گرفتن راه هایی برای مقابله با اینگونه سوء استفاده ها احساس میگردد. به همین دلیل امروزه تلاش های بسیاری برای ارائه روش های تشخیص و مقابله با نفوذ صورت میگیرد . با پیشرفت تکنولوژی , همانگونه که نحوه و چگونگی فعالیت های نفوذی تغییر نموده , انتظارات از سیستم های تشخیص نفوذ نیز افزایش یافته است . دسته مهمی از سیستم های تشخیص نفوذ از روش هی

یادگیری برای مدل نمودن نفوذ استفاده می نمایند.روش های جدید در حملات به سیستم های کامپیوتری توجه محققین را به سمت خود جلب نموده است . سیستم تشخیص نفوذ تلاشی است در جهت کشف حمله کننده و یافتن روش هایی که این گونه افراد در جهت نفوذ به اطلاعات کامپیوتری به کار میگیرند . از نظر کل این مورد بسیار اهمیت دارد که در برابر چنین حملات و تهاجماتی ایستادگی نمود . ولیکن بدون طراحی بنیادین یک راه حل مبتنی بر این سیستم جهت جستجوی حملات امکان پذیر نمی باشد.امروزه برای تشخیص حملات روی شبکه های مهمی چون شبکه های بیسیم , نیاز به نرم افزارهای هوشمند تری داریم , زیرا که یک هکر باهوش همیشه برای مخفی کردن حملاتش , راه های هوشمندانه ای را انتخاب میکند . مهاجمین ممکن است که از تکنیک های مخفی سازی استفاده کنند که بسیاری از سیستم های تشخیص نفوذ در حال حاضر توانایی شناسایی آنها را ندارند . به طور قطع تشخیص یک حمله کار بسیار مشکلی می باشد و یا اینکه پس از تشخیص حمله , امکان شناسایی نوع حمله و آنکه مهاجم چه کاری انجام میدهد دشوار تر است و در کل آنکه برای تشخیص و ارائه عملکرد مناسب نیاز به تکنیک های پیچیده تر و هوشمندانه تری داریم . بنابر این نیاز به رویکردی جدید در خصوص هوشمند سازی سیستم تشخیص نفوذ امری الزامی است . به طور کلی روشهای متعددی برای هوشمند سازی این سیستم ها پیشنهاد شده و در حال تحقیق و توسعه است که از آن جمله میتوان به استفاده از الگوریتم های ژنتیک , سیستم های خبره ,منطق فازی و شبکه های عصبی اشاره نمود.در این تحقیق از تکنیک داده کاوی و الگوریتم های یادگیری ماشینی برای هوشمند سازی , نرم افزار snort برای تشخیص نفوذ و از یک پایگاه داده تولید شده بر اساس حملات جدید برای ارزیابی آن ها استفاده شده است . ویژگی استخراج شده از داده ها شامل ویژگی شخصی ارتباط , ویژگی های ترافیکی زمانی و تعدادی ویژگی های معنایی می باشند . داده های موجود در این پایگاه داده در یکی از دسته های normal,U2R,R2L,DOS,probe قرار میگیرند.

نفوذ و عوامل نقوذ

نفوذ, مجموعه اقدامات غیر قانونی است که صحت, محرمانگی یا دسترسی به یک منبع را به خطر می اندازد. به طور کلی نفوذ را میتوان به دسته های زیر تقسیم نمود:

- ورود غیر قانونی: هنگامی اتفاق می افتد که یک بیگانه به شناسه کاربری و رمز عبور دسترسی پیدا می کند.
- حملات فریبکارانه زمانی اتفاق می افتد که نفوذگر سیستم را متقاعد می کند که او یک کاربر مجاز است.
- نفوز به سیستم کنترل امنیت: نوذگر تلاش می کند که موارد امنیتی سیستم را تصحیح نماید.
- نشت: زمانی است که اطلاعات به خارج سیستم منتقل می شود.
- جلوگیری از ارائه سرویس: زمانی ست که منابع برای سایر کاربران دسترس ناپذیر می شود.
- استفاده های خراب کارانه: شامل حملاتی از قبیل حذف فایل ها و سوء استفاده از منابع می باشد.

روش های نفوذ به شبکه های کامپیوتری

الف- استفاده از عیوب نرم افزاری : با توجه به اینکه در تولید نرم افزار ها به روش های غیر رسمی و غیر استاندارد نمی توان تمامی خطاهای موجود در آن ها را تشخیص داد و تنها از طریق تولید آن با روش های رسمی و فرمال ریاضی می توان به خطاها دست یافت. اما چون استفاده از روش های رسمی مشکل, زمان بز و دارای هزینه زیادی است, معمولا شرکت های تولید کننده از روش های رسمی استفاده نمی کنند و این امر باعث شده که همواره در نرم افزار ها نقاط ضعف هایی وجود داشته باشد. عیوب نرم افزاری را می توان به صورت زیر بیان نمود:

- سرریز شدن بافر: برنامه نویسان از بافر ها در برنامه های خود برای وارد نمودن داده های معتبر خود استفاده می کنند. حال اگر داده های اضافی بیش از آن که برای برنامه در نظر گرفته شده است در این بافر ها وارد شود, سرریز اتفاق می افتاد و در نتیجه ناحیه دیگر از حافظه که برای نگهداری دستورالعمل های برنامه در نظر گرفته شده بود, بازنویسی می شود. نفوذگران با دستکاری جایی که این داده های اضافی خاتمه می پذیرند می توانند باعث اجرای فرمان هایی توسط سیستم عامل شوند.

- ترکیبات غیر منتظره: برنامه ها معمولا با استفاده از چندین لایه کد ساخته می شوند که سیستم عامل پایین ترین لایه آن است. گاهی اوقات نفوذگران درخواستی را می فرستند که برای یک لایه بی معنی, اما برای لایه های دیگر معنی دار است و منجر به اجرای عملی می شود.

ب- شکستن کلمه عبور : معمولا برای این کار از روش های زیر استفاده می شود:

- حدس زدن کلمات عبور: معمولا مردم از نام های خودشان, فرزندان, دوستان و مدل های ماشین ها برای کلمه عبور استفاده می کنند بنابراین حدس کلمه عبور به راحتی امکان پذیر است.
- حملات واژه نامه ها: در صورت عدم موفقیت حدس کلمه عبور, نفوذگران می توانند با استفاده از یک برنامه تمام کلمات موجود در واژه نامه را امتحان کنند.
- حملات Brute Force: یک کلمه عبور چهار حرفی که فقط حاوی حروف کوچک است, می تواند در عرض کمتر از چند دقیقه شکسته شود در حالیکه کلمات هفت کاراکتری که از ترکیب حروف کوچک و بزرگ همراه با اعداد و نشانه هاست ممکن است ماه ها وقت بخواهد تا شکسته شود.

ج- استراق سمع ترافیک نا امن : نفوذ گر ها با نصب یک استراق سمع کننده روی هر قسمت شبکه, می توانند ترافیک شبکه را که از آن قسمت شبکه عبور می کند را ضبط نموده و از اطلاعات به دست آمده برای ورود به شبکه استفاده کند.

د- استفاده از نقاط ضعف طراحی:

- نقاط ضعف پروتکل TCP/ IP: چون زمانی که این پروتکل طراحی شد نفوذ به شبکه های کامپیوتری در مقیاس وسیع امروزی وجود نداشت, بنابراین طراحی این پروتکل دارای نقاط ضعف زیادی می باشد که منجر به بروز مشکلات امنیتی زیادی شده است.
- نقاط ضعف طراحی سیستم عامل یونیکس: نقطه ضعف ذاتی در طراحی این سیستم عامل وجود دارد که منتهی به نفوذ در آن می شود.

روش های تشخیص نفوذ به شبکه های کامپیوتری

- تشخیص رفتار غیر عادی :به منظور تشخیص رفتار غیر عادی می توان ابتدا نماهایی از رفتارهای عادی هر یک از کاربران ایجاد کرد, سپس رفتار فعلی کاربران را با این نماها مقایسه کرد و در صورت بروز هرگونه مغایرت رفتار غیر عادی را به مسئول امنیتی سیستم اطلاع داد.

نماهای رفتار ادی کاربران به صورت مجموعه ای از معیارهای قابل اندازه گیری تعریف می شود. این معیارها جنبه های به خصوصی از رفتار کاربران هستند. به طور کلی استفاده روزانه کاربران از یک سیستم کامپیوتری از الگوهای رفتاری قابل تشخیص پیروی می کند.

- تشخیص سوء استفاده :ایده اصلی در تشخیص سوء استفاده اینست که روش هایی وجود داشته باشد که به کمک آن ها بتوان هر نفوذ را در قالب یک الگو نمایش داد به طوری که انواع متفاوتی از همان نفوذ قابل شناسایی باشد. این مساله به واسطه دامنه ساده موضوعاتی که الگو یا مدل شده اند, می تواند به سطح بالایی از صحت و دقت دست پیدا کند.

سیستم های تشخیص نفوذ

در مبحث امنیت کامپیوتر و شبکه, سیستم های تشخیص نفوذ در نقش هشدار دهنده هستند و هر زمان که امنیت شبکه در معرض خطر قرار گیرد آن را اعلام می کنند. سیستم تشخیص نفوذ, یک سیستم محافظتی است که خرابکاری های در حال وقوع روی شبکه را شناسایی می کند. روش کار به این صورت است که با استفاده از تشخیص نفوذ که شامل مراحل جمع آوری اطلاعات, پویش پورت ها, به دست آوری کنترل کامپیوتر ها و نهایتا هک کردن می باشد, می تواند نفوذ خراب کاری ها را گزارش و کنترل کند. از قابلیت های دیگر این سیستم, امکان تشخیص ترافیک غیر متعارف از بیرون به داخل شبکه و اعلام آن به مدیر شبکه است.

اهداف سیستم های تشخیص نفوذ

تشخیص رفتار غیر عادی از جمله اهداف اولیه تشخیص نفوذ می باشد. دومین هدف جمع آوری داده ها بر اساس رفتار سیستم, تسهیل بازیابی سیستم پس از نفوذ است. این اهداف به صورت عمده می تواند به شکل زیر بیان شود:

- باید توانایی تشخیص رفتار عادی یک کاربر را از رفتار غیر عادی داشته باشد.
- باید توانایی اداره ساختارهای پیچیده و فعل و انفعالات موجود در شبکه های نا همگون را داشته باشد.
- توانایی قرار گرفتن در شبکه های متنوع و معماری های مختلف سیستم را داشته باشد.
- توانایی تطبیق و انطباق در پاسخ به حملات جدید و الگوهای به کار رفته را داشته باشد.
- توانایی حملات را به صورت بلادرنگ داشته باشد و به محض اینکه اتفاق افتاد مدیر امنیتی شبکه را خبردار کند.
- باید بتواند از خود در مقابل حملات مراقبت کند.
- می بایستی قابلیت همکاری با مکانیزم های دیگر امنیتی جهت افزایش امنیت در سیستم ها را داشته باشد.

معماری سیستم های تشخیص نفوذ

سیستم های تشخیص نفوذ دارای یک معماری بسیار ساده هستند که معمولا شامل چهار بخش زیر می باشند.

- **حس گر:** ترافیک شبکه, گزارش کارها و یا رفتار سیستم را دنبال می کند و از این طریق داده ها را به رویدادهای قابل استفاده برای ناظران سیستم های تشخیص نفوذ تبدیل می کند.
- **ناظر:** رویدادها را از حسگر ها دریافت می کنند سپس آن ها در مدل رفتاری سیستم تشخیص نفوذ با هم در ارتباط قرار می گیرند. عامل باالقوه هشدارها, اطلاعات به روز مدل ها را شکل می دهد, هشدارها و رخدادهای قابل اهمیت برای امنیت یک سیستم را نشان می دهد و به ناظران سطح بالا یا واحد های تبدیل کننده ارسال می کنند.
- تبدیل کننده: اجزای تبدیل کننده گزارشات تردید آمیز را از ناظران(به شکل یک هشدار) دریافت و پاسخ مناسب به صورت گزارش تغییر رفتار اجزای سطح پایین تر صادر می کند.
- کنترل کننده :این واحد ها محل منحصر به فرد سرپرستی و باز پرسی برای سیستم های تشخیص نفوذ هستند و می توانند به صورت یک بازپرس عمل کرده و اجزای نا موفق را دوباره به کار می اندازد.

انواع سیستم های تشخیص نفوذ

- سیستم های تشخیص نفوذ مبتنی بر میزبان :در این سیستم ها یک عامل هوشمند بر روی میزبان نظارت شده نصب می شود. این کارگزار جنبه های متفاوتی از امنیت میزبان, از قبیل فایل های رخدادهای سیستم عامل, فایل های رخداد های کاربردی را زیر نظر می گیرد. برخی از سیستم های تشخیص نفوذ مبتنی بر میزبان به صورت توزیع شده عمل می کند. در این سیستم ها, اطلاعات از چندین میزبان جمع آوری شده و به یک میزبان مرکزی ارسال می شود و تحلیل حملات پیچیده تر در این میزبان مرکزی انجام می شود.

در این سیستم ها از ترافیک شبکه به عنوان منبع اصلی اطلاعات استفاده می شود. معمولا کارت وسط شبکه قادر است ترافیک شبکه ای را که از آن عبور می کند ملاحظه نماید.

این سیستم های تشخیص نفوذ برای کاربران شبکه شفاف هستند و احتمال کمی وجود دارد که دشمن بتواند آن ها را جایگزین کند و یا قابلیت هایش را بدون کوشش قابل ملاحظه ای کاهش دهد.

- سیستم های تشخیص نفوذ مبتنی بر شبکه :در این سیستم ها از ترافیک شبکه به عنوان منبع اصلی اطلاعات استفاده می شود. معمولا کارت واسط شبکه قادر است ترافیک شبکه ای را که از آن عبور می کند ملاحظه نماید.

این سیستم های تشخیص نفوذ برای کاربران شبکه شفاف هستند و احتمال کمی وجود دارد که دشمن بتواند آن ها را جایگزین کند و یا قابلیت هایش را بدون کوشش قابل ملاحظه ای کاهش دهد.

- سیستم های تشخیص نفوذ مبتنی بر میزبان و شبکه :این سیستم ها تلفیقی از دو سیستم فوق هستند. که از منابع اطلاعاتی میزبان و هم از منابع اطلاعاتی شبکه برای تشخیص نفوذ استفاده می شود.

محدودیت های سیستم های تشخیص نفوذ

۱. مهاجم یاب داخلی به تنهایی نمی تواند کاری انجام بدهد و فقط یک تشخیص دهنده است و نیاز به همکاری سایر ابزارهای امنیتی مانند دیواره آتش دارد.

۲. مهاجم یاب داخلی نمی تواند جانشین سیاست های امنیتی و برنامه ریزی بشود بلکه خود باید بر اساس سیاست های امنیتی تنظیم گردد.

۳. False Positive در برابر False Negative

- False Positive: زمانی که یک سیستم تشخیص نفوذ و وقوع یک نفوذ را گزارش می دهد ولی واقعا اتفاق نیفتاده است, این نوع خطا رخ می دهد. این نوع خطا می تواند مشکلاتی را به دنبال داشته باشد, به عنوان مثال وقوع هشدارهای متعدد می تواند راهبرد را نسبت به این سیستم بی اعتماد کند.
- False Negative : زمانی که نفوذ رخ داده ولی سیستم تشخیص نفوذ آن را گسترش نداده است و در تشخیص آن ناتوان بوده است, این خطا رخ می دهد. خطای خطرناکی است و می تواند راه نفوذ به شبکه را فراهم آورد.

معرفی چند نمونه سیستم تشخیص نفوذ

Computer Watch: یک سیستم تشخیص نفوذ مبتنی بر میزبان است که امکانات پرس و جو و گزارش متعددی را برای مسئول امنیتی فراهم می کند. از یک سیستم خبره استفاده می شود تا وقایع مربوط به امنیت را خلاصه کند و یک تحلیل گر آماری و مکانیزم پرس و جو, مشخصه های آماری وقایع سیستم را فراهم می کند.

NIDES: یک سیستم تشخیص نفوذ است که داده های ردیابی, از یک یا چند میزبان جمع آوری شده و به یک کیزبان مرکزی فرستاده می شود. هم تحلیل مبتنی بر قانون و هم تحلیل آماری بر روی این داده ها انجام می شود. نتایج تحلیل شده و به اطلاع مسئول امنیتی سیستم رسانده می شود.

NSM: این سیستم را باید نقطه عطفی در توسعه سیستم های تشخیص نفوذ دانست به این دلیل که این سیستم اولین تلاش برای گسترش نفوذ به شبکه های نا همگون بود.

GRIDS: این سیستم بر اساس پیاده سازی رفتار شبکه بر روی گراف ها می باشد. این گراف ها به صورت سلسله مراتبی از جائیکه شروع می شوند تا زیر سیستم ها که به گره های تکی در گراف ختم می شوند پیاده سازی می گردد و یک تراکنش بین نقاط همتا در یک سطح مدل می شود. با نگهداری گره های خارجی از یک گره به گره های دیگر یک تصویر را از رفتار شبکه بیان می کند.

OSSEC: این سیستم یکی از شناخته شده ترین سیستم های تشخیص نفوذ مبتنی بر میزبان است که توسط Daniel Cid طراحی, تولید و توسعه یافته است. دلیل اصلی استفاده از این نرم افزارمنبع باز بودن آن و عملکرد مناسب آن است. از دیگر مزیت های آن می توان به موارد ذیل اشاره کرد:

- با اکثر سیستم عامل ها از جملهSolaris, Mac OSX, MS Windows Open BSD, Free BSDو Linux سازگار بوده و قابل نصب بر روی آن هاست.
- این توانایی را دارد که با قرار گرفتن در کنار یک حفاظ به صورت خودکار, تلاش هایی که جهت نفوذ به سیستم سرویس دهنده انجام می گیرند را مسدود کند.
- عامل های این سیستم این توانایی را دارند که آدرس IP سیستم مورد استفاده مهاجمان را ذخیره کنند و بسته هایی که در این آدرس ها دریافت می شوند را حذف کنند, سپس از این آدرس ها در حفاظ استفاده کنند. OSSEC از حفاظ های مختلف مبتنی بر سیستم عامل ویندوز و لینوکس پشتیبانی می کند.
- این توانایی را دارد که فعالیت های غیر عادی و غیر معمول شبکه را از طریق پست الکترونیکی به مدیر شبکه اطلاع دهد.
- انعطاف پذیری قوانین در این نرم افزار بسیار زیاد می باشد, به گونه ای که این توانایی را به مدیر شبکه می دهد که به طور کامل هشدار ها و قوانین را با توجه به سیاست های امنیتی خود تغییر دهد.

- قابلیت و توانایی تشخیص این سیستم صرفا معطوف به قوانین نمی باشد بلکه از طریق بررسی فایل های ثبت رویداد ها می تواند بسیاری از تغییرات انجام گرفته در میزبان تحت نظارت را تشخیص دهد.
- توانایی کنترل و نمایش اغلب کرم های اینترنتی, نرم افزار های جاسوسی و درب پشتی که در رجیستری ویندوز رخنه کرده اند, را دارا می باشد.
- این توانایی را دارد که فایل های رمز شده به کمک الگوریتم های MD5 و SHA1 را بررسی کند.
- با بررسی رخداد های مربوط به کاربرانی که با سطح دسترسی مدیر در حال فعالیت می باشند, می تواند رفتار های غیر عادی انواع Rootkit در سطح هسته و دیگر حملات از این قبیل را تشخیص دهد.
- این قابلیت را دارد که با اجرای برخی دستورات در سطح سیستم, به حملاتی که تشخیص داده شده اند, پاسخ دهد.
- به طور کامل از نرم افزار NMAP پشتیبانی می کند و می تواند با این نرم افزار به صورت کامل در شناسایی تعامل داشته باشد.

Snort: این ابزار ترافیک شبکه را ربوده و به روش های مناسبی غربال کرده و در یک فایل ذخیره می نماید. در این نرم افزار قابلیت اسکریپت نویسی وجود دارد که به آن انعطاف پذیری بسیار بخشیده است.

Snort یک نرم اافزار تشخیص نفوذ به صورت کد باز است که بر روی محیط های Linux و Windows عرضه می گردد و با توجه به رایگان بودن آن, به یکی از متداول ترین سیستم های تشخیص نفوذ شبکه های رایانه ای مبدل شده است.

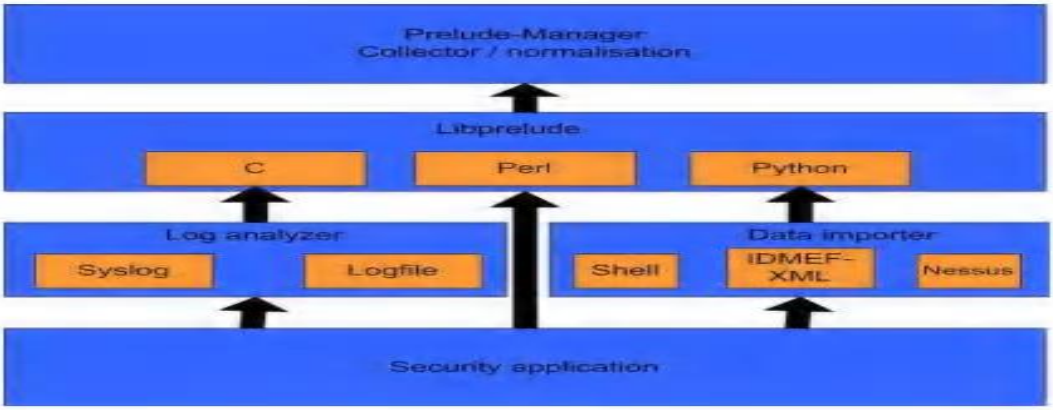
این نرم افزار در سه حالت قابل برنامه ریزی است:

- حالت Sniffer : در این حالت, این نرم افزار تنها یک استراق سمع کننده ساده است و محتوای بسته های رد و بدل شده بر روی شبکه را بر روی کنسول نمایش می دهد.
- حالت ثبت کننده بسته ها :در این وضعیت, اطلاعات بسته های شبکه را در در پرونده ای که مشخص می شود ذخیره می کند.
- سیستم تشخیص نفوذ :در این پیکر بندی, بر اساس دو قابلیت پیشین و با استفاده از قابلیت تحلیل بسته ها و قوانینی که تعیین می گردد, Snort امکان پایش و تحلیل بسته و تشخیص نفوذ را یافته و در صورت نیاز واکنش تعیین شده را بروز می دهد.

حالت پیش فرض خروجی این نرم افزار فایلی متنی است که می تواند در آن بسته ها را نیز درج کند. با این وجود در صورتی که این ابزار در حال فعالیت بر روی ارتباطات شبکه ای با سرعت بالا می باشد بهترین راه استفاده از خروجی خام باینری و استفاده ابزاری ثانویه برای تحلیل و تبدیل اطلاعات خروجی است. بعد دیگر پیکر بندی Snort به عنوان یک سیستم تشخیص نفوذ, استفاده از قوانین برای ایجاد معیار نفوذ برای Snort است. برای مثال می توان با قانونی, آن را مکلف ساخت که نسبت به دسترسی های انجام شده مبتنی بر پروتکلی تعیین شده از (به یک پورت خاص و از) به یک مقصد معین با محتوایی شامل رشته ای خاص, اخطاری یا واکنشی ویژه را اعمال کند.

Prelude: با ارائه انواع سیستم های تشخیص نفوذ, که هر یک از آن ها خصوصیات منحصر به فرد مربوط به خود را دارند,Prelude نیز جهت یکپارچه کردن اطلاعات مربوط به هر سیستم تشخیص نفوذ در یک بانک اطلاعاتی جامع ارائه شد. با جمع آوری اطلاعات امنیتی از تحلیل رهای مختلف و یکپارچه کردن این اطلاعات می توان محصول امنیتی بسیار قوی تولید کرد. در حقیقت, این سیستم دارای ساختار ترکیبی از سیستم های تشخیص نفوذ می باشد که اطلاعات را از هر سیستم دریافت, و به سیستم مرکزی تحویل می دهد. Prelude به منظور ترکیب اطلاعات سیستم های تشخیص نفوذ متفاوت از استاندارد IDMEF استفاده می کند که حسگر های مختلف را قادر می سازد رویداد هایی با یک زبان واحد ایجاد کنند.

Prelude توسط سه زبان ,Perl C و Python چارچوبی را جهت قابل فهم نمودن اطلاعات دریافت شده از حسگر های مختلف, ارائه می دهد. همچنین حسگرهایی مانند Prelude LML که قادر به استفاده از چارچوب Prelude می باشند را برای مدیر شبکه فراهم می کند. شکل ۲-۲- ساختار فنی این سیستم را نشان میدهد.



ساختار فنی Prelude

مقایسه سیستم های تشخیص نفوذ

یک سیستم تشخیص نفوذ مبتنی بر شبکه, توانایی بیشتری در دریافت بلادرنگ بسته ها و عملیات تجزیه و تحلیل بر روی آن ها را دارد. بسیاری از توانایی های موجود در یک سیستم تشخیص نفوذ مبتنی بر شبکه را نمی توان به راحتی در سیستم های تشخیص نفوذ مبتنی بر میزبان به دست آورد. برخی از این قابلیت ها عبارتند از:

- **هزینه مالکیت** :سیستم ها تشخیص نفوذ مبتنی بر شبکه بر خلاف سیستم های تشخیص نفوذ مبتنی بر میزبان, بدون نصب نرم افزارهای مدیریتی اضافی, اجاره نظارت بر نقاط بحرانی را می دهند. بدین ترتیب هزینه مدیریت برای محیط های بزرگ به شدت کاهش می یابد.
- **تحلیل بسته ها** :سیستم های تشخیص نفوذ مبتنی بر شبکه, تمام سرآیند بسته ها را برای یافتن فعالیت های مشکوک و مغرضانه مورد جستجو و امتحان قرار می دهند. بسیاری از حملات جلوگیری از سرویس مبتنی بر IP با جستجو در سرآیند بسته ها قابل شناسایی هستند.
- **حذف شواهد** :سیستم های تشخیص نفوذ مبتنی بر شبکه از ترافیک شبکه, به صورت بلادرنگ, جهت شناسایی حمله ها استفاده می کنند و هرگز یک مهاجم نمی تواند شواهد دریافتی, از روند انجام حمله را حذف کند. در مورد سیستم های تشخیص نفوذ مبتنی بر میزبان تجربه نشان داده است اولین اقدامی که یک مهاجم جهت از بین بردن رد پای خود انجام می دهد, حذف و یا آسیب رساندن به فایل های ثبت رخداد می باشد.
- **تشخیص و پاسخ گویی بلادرنگ** :سیستم های تشخیص نفوذ مبتنی بر شبکه این قابلیت را دارند که در کمترین زمان ممکن, حمله های مشکوک را شناسایی و پاسخ ها و هشدار های مناسبی را در مورد آن ها صادر کنند.
- **شناسایی تلاش های مغرضانه** :اگر یک سیستم تشخیص نفوذ مبتنی بر شبکه را در محلی خارج از محدوده تشخیص یک حفاظ قرار دهیم, سیستم می تواند حمله هایی را که هدفشان منابع پشت حفاظ می باشند, شناسایی کند. چون این حمله ها با هیچ میزبانی برخورد مستقیم نداشته اند, بنابر این سیستم تشخیص نفوذ مبتنی بر میزبان توانایی تشخیص این نوع حملات را ندارند.
- **مکمل سایر اجزای امنیتی** :سیستم های تشخیص نفوذ مبتنی بر شبکه می توانند به عنوان مکمل اجزای امنیتی شبکه نیز مطرح می شوند. برای نمونه این سیستم ها نمی توانند تمامی داده های رمزنگاری شده را در ترافیک شبکه بخوانند ولی این قابلیت را دارند که اطلاعات رمزگذاری نشده در ترافیک شبکه را مشخص کنند. سیستم های تشخیص نفوذ مبتنی بر شبکه می توانند آدرس ها و یا ترافیک مربوط به مهاجمان را تشخیص داده و آن ها را در اختیار حفاظ قرار دهند تا حفاظ از این به بعد ترافیک دریافتی از این آدرس ها را مسدود کند.
- **استقلال از سیستم عامل** :سیستم های تشخیص نفوذ مبتنی بر شبکه به طور کلی از سیستم عامل های میزبان کاملا مستقل می باشند. این در حالی است که سیستم های تشخیص نفوذ مبتنی بر میزبان به سیستم عامل میزبان وابسته اند و در صورت از کار افتادن سیستم عامل قادر به ادامه فعالیت خود نیستند.

با توجه به مزیت سیستم های تشخیص نفوذ مبتنی بر شبکه نسبت به سیستم های مبتنی بر میزبان تصمیم به استفاده از یک سیستم مبتنی بر شبکه گرفته شد که از این بین Snort انتخاب می شود که می تواند به عنوان یک سیستم تشخیص و جلوگیری از نفوذ مورد استفاده قرار گیرد و خصوصیات آن در فصل بعدی به طور کامل بررسی می شود.

بررسی کارهای انجام شده و مقالات داخلی

در پایان نامه "طراحی و پیاده سازی یک سیستم تشخیص نفوذ با استفاده از تکنیک های داده کاوی "هدف پروژه طراحی و پیاده سازی یک سیستم تشخیص نفوذ با استفاده از تکنیک های داده کاوی است . در این راستا اهداف و مشخصات سیستم های IDS مورد بررسی قرار گرفته اند , سپس با نگاشت مساله تشخیص نفوذ به یک مساله دسته بندی دو یا چند کلاسی ظع سعی شده است تا مساله از این طریق حل شود . با توجه به حجم بالای داده های درگیر در مسائل تشخیص نفوذ , روش های کلاسیک دسته بندی , به سادگی , قادر به حل این مساله نمیباشند. روش جدیدی مبتنی بر قوانین انجمنی فازی برای دسته بندی ارائه گردیده است . در این روش از مجموعه های قوانین انجمنی فازی به عنوان مدل های توصیف کننده کلاس های مطرح در مساله استفاده میشود. برای برچسب گذاری نمونه های آزمایشگاهی , میزان سازگاری هر نمونه با مجموعه قوانین متفاوت تخمین زده میشود . کلاس نتناظر با مجموعه قانونی که بیشترین سازگاری را با نمونه مورد بحث داشته باشد به عنوان برچسب نمونه انتخاب میشود . با توجه به پایین بودن سرعت الگوریتم های استخراج قوانین انجمنی , راهکارهایی نیز برای افزایش سرعت این الگوریتم ها ارائه شده و سناریوهای متفاوتی برای بکارگیری روش دسته بندی پیشنهادی در حوزه تشخیص نفوذ ارائه شده است . اغلب این سناریوها مبتنی بر تشخیص سوئاستفاده عمل میکنند درحالیکه یک سناریوی مبتنی بر تشخیص ناهنجاری نیز ارائه گردیده است . برای ارزیابی روشهای ارائه شده برای تشخیص نفوذ,از مجموعه داده KDD99 استفاده شده است.

در "تشخیص نفوذ با استفاده از مدل مخلوط گوسی و مقایسه و ترکیب آن با ماشین بردار پشتیبان" سعی میشود تا با استفاده از مدل مخلوط گوسی و ماشین بردار پشتیبان نسبت به تشخیص نفوذ اقدام گردد. از آنجا که نواحی خطای این دو روش لزوما دارای هم پوشانی کامل نیستند , نسبت به ترکیب بهینه این دو روش در راستای کاهش میزان خطا و افزایش کارایی در تشخیص نفوذ اقدام شده است . تکنیک مدل مخلوط گوسی یک روش یادگیری از نوع مولد می باشد . در این روش , هریک از دسته های ورودی به تنهایی و بدون مقایسه با سایر دسته ها ,مدل میشود . در این روش سعی میشود تا توسط مجموعه ای از توابع توزیع احتمال گوسی که آنها را مخلوط های گوسی می نامیم بهترین توزیع احتمال ممکن برای هر دسته ساخته شود. تعداد مخلوط ها در هر مدل و میانگین و واریانس هر یک از انها , اثرات متفاوتی بر کارایی این روش دارد. تکنیک ماشین بردار پشتیبان یک الگوریتم تمایزی می باشد. در این تکنیک هر مدل ماشین بردار پشتیبان وظیفه طبقه بندی دو یا چند دسته (کلاس) از داده های ورودی را برعهده میگیرد و بر اساس توزیع داده های ورودی و مقایسه آنها , یک ابر صفحه برای جداسازی این دسته ها پیشنهاد مینماید . جداسازی دسته ها با توجه به پراکندگی آنها از مزایای این روش می باشد .این تکنیک به عنوان یک جداساز بهینه کارایی خوبی رادر طبقه بندی داده ها در کاربردهای مختلف از خود نشان داده است . در این پروژه تکنیک های مدل مخلوط گوسی و ماشین بردار پشتیبان برای تشخیص نوع نفوذ از پایگاه داده KDD-99 برای ارزیابی آن ها استفاده شده است . ویژگی های استخراج شده از داده ها شامل ویژگی های شخصی ارتباط, ویژگی های ترافیکی زمانی و تعدادی و ویژگی های معنایی می باشد . مجموعا ۴۱ ویژگی از داده ها استخراج میشود . داده های موجود در این پایگاه داده در یکی از دسته های DOS,R2L,U2R,Noral,Probe قرارمیگیرند . انتخاب ویژگی ها, یکی از مشکلات سیستم های تشخیص نفوذ می باشد . در تست های انجام گرفته در ساخت سیستم های تشخیص نفوذ با استفاده از مدل مخلوط گوسی , کارایی ویژگی های مختلف مورد بررسی قرارگرفته است . استفاده از ویژگی هایی که از داده های جابجا شده در طول هر ارتباط بدست می آید , در تشخیص حملات U2R,R2L,DOS و وضعیت Normal کارایی دارد. از تمامی ویژگی ها برای تشخیص Probe از سایر دسته ها استفاده شده است. تکنیک مدل مخلوط گوسی در تشخیص دسته هایی که دارای رکورد های آموزشی کافی هستند , کارایی خوبی دارد. این تکنیک در تشخیص حملات ناشناخته بدلیل پایین بودن قدرت تعمیم آن , ضعیف عمل می کند. یکی از تکنیک های استفاده شده در این پروژه برای تشخیص نفوذ , ماشین بردار پشتیبان می باشد. درتست های انجام شدهاز تمامی ۴۱ ویژگی , در این تکنیک استفاده شده است . برای کاهش حجم داده های آموزشی و در نتیجه افزایش سرعت آموزش سیستم , هم از کوانتیزاسیون و هم از انتخاب اتفاقی بردارها استفاده شده است . در دسته های Normal,DOS که تعداد رکوردهای آموزشی زیاد است , کوانتیزاسیون برداری و در سایر دسته ها انتخاب اتفاقی رکوردها کارایی بالاتری دارند. از آنجا که تکنیک ماشین بردار پشتیبان یک تکنیک

تمایزی است , این تکنیک از قدرت تعمیم بالاتری برخوردار می باشد و قادر است حملات ناشناخته را نیز تشخیص دهد. مدل مخلوطی گوسی در تشخیص دسته های Normal,DOS که از تعداد رکوردهای آموزشی زیادی برخوردار است , کارایی بالاتری نسبت به ماشین بردار پشتیبان دارد. در صورتیکه ماشین بردار پشتیبان در تشخیص U2R , U2L و Probe کارایی بالاتری دارد . از آنجا که نواحی خطای این دو روش لزوما دارای هم پوشانی کامل نیستند , نسبت به ترکیب بهینه این دو روش در راستای کاهش میزان خطا و افزایش کارایی در تشخیص نفوذ اقدام شده است . سیستم ترکیبی دارای سه مرحله پردازش است . در مرحله اول با استفاده از مدل مخلوط گوسی وضعیت Prob از سایر دسته ها تشخیص داده می شود . در مرحله دوم , در صورتیکه نوع وضعیت Prob نباشد , با استفاده از تکنیک مدل مخلوط گوسی یکی از دسته های Normal ,U2R,R2L و DOS به عنوان خروجی انتخاب می شود . از آنجا که در تشخیص U2R و Probe بیشترین میزان خطا وجود دارد از ماشین بردار پشتیبان برای تصحیح خروجی در این دو حالت استفاده می شود .

در " بررسی صحت عملکرد سیستم های تشخیص نفوذ توسط عامل های متحرک " , به کارگیری جزئی به نام بازرس برای سیستم های تشخیص نفوذ بررسی شده اند . برای بازرس سه معماری کلی پیشنهاد شده است که آنها را بازرس محلی , بازرس متمرکز و بازرس متحرک نامیده اند . سپس این سه معماری بازرس از نظر زمان پاسخ , میزان بار شبکه و میزان بار سیستم با یکدیگر مقایسه شده اند . علاوه بر این موارد معیار دیگری را نیز تحت عنوان قابلیت پیکربندی مجدد سیستم در نظر گرفته شده است و نتایج حاصل از آزمایشات نشان داده که عملکرد بازرس محلی در مقایسه با دو نمونه دیگر دارای زمان پاسخ کمتر و همچنین بار کمتر دارد . این نتیجه نشان می هد که استفاده از بازرس محلی در شبکه های کوچک مناسب است . علت اینکه به کارگیری بازرس محلی برای شبکه های کوچک مناسب است , مساله پیکربندی مجدد بازرس ها می باشد . در صورتیکه لازم باشد بعد از مدتی پیکربندی و نحوه عملکرد بازرس ها تغییر کند , در صورت استفاده از بازرس محلی لازم است که بر روی تک تک سیستم ها این تغییرات را ایجاد کرد , که انجام این کار در صورت وسعت شبکه کاری سخت و وقتگیر است . با توجه به این مطلب , برای شبکه های بزرگ , استفاده از بازرس متحرک به عنوان روش مناسب پیشنهاد می شود . در این روش کافیست که تغییرات را بر روی بازرسی که در شبکه رها می شود , اعمال کرد . استفاده از بازرس متمرکز نیز به علت بار زیادی که بر روی شبکه و سیستم می گذارد , روش مناسبی نمی باشد . با انتخاب بازرس متحرک به عنوان روش برگزیده برای شبکه های بزرگ , دو پارامتر را در مورد آنها بررسی کردیم . این دو پارامتر عبارتند از تعداد بازرس های متحرک در شبکه و نحوه حرکت آن ها . برای بررسی این دو پارامتر معیاری تعریف کردیم به صورت حاصل ضرب بار شبکه در زمان پاسخ . هرچه که تعداد بازرس های ارسالی بر روی شبکه بیشتر باشد , میزان ترافیک شبکه افزایش پیدا می کند , اما بازرسی های مورد نظر سریعتر انجام می شود و زمان پاسخ کاهش می یابد و بالعکس . با توجه به این مساله که این دو پارامتر (بار شبکه و زمان پاسخ) نسبت عکس با یکدیگر دارند , حالتی را باید پیدا کرد که حاصل ضرب این دو به صورت بهینه و حداقل باشد . با بررسی آزمایشات صورت گرفته مشخص شد که در صورتیکه شبکه به بخش هایی با میزبان مساوی شکسته شود , میزان بار شبکه در زمان پاسخ حداقل خواهد شد .

در " تشخیص سلسله مراتبی نفوذ به روش ناهنجاری به وسیله شبکه های عصبی" یک سیستم تشخیص نفوذ سلسله مراتبی طراحی و پیاده سازی شده است که قادر است حملات مبتنی بر شبکه را با روش تشخیص ناهنجاری و به وسیله شبکه های عصبی تشخیص دهد . شبکه های عصبی به دلیل دارا بودن توانایی دسته بندی بالا و قدرت تعمیم می توانند در سیستم های تشخیص نفوذ به کار برده شوند . شبکه نمونه از سه سطح سلسله مراتب استفاده می کند که هر سیستم تشخیص نفوذ در سطح پایین , گزارشی را به سیستم تشخیص نفوذ در سطح بالا ارسال می کند . این سیستم تشخیص نفوذ با دریافت بسته ها از شبکه , ویژگی های اتصالات شبکه را استخراج کرده و پس از پیش پردازش آماری بر روی اتصالات با استفاده از دسته بندی شبکه های عصبی رفتارهای غیرعادی را در سطح شبکه تشخیص می دهد . سیستم تشخیص نفوذ پیاده سازی شده از شبکه های عصبی در ساختار خود به عنوان دسته بندی کننده استفاده می کند که سیستم های تشخیص نفوذ سلسله مراتبی و توزیع شده کنونی فاقد چنین ویژگی هستند . شبکه های عصبی مورد استفاده BP و PBH (هیبرید پرسپترن و BP) می باشند که شبکه عصبی PBH تا کنون در یک محیط واقعی مورد آزمایش قرار نگرفته است و الگوریتم یادگیری شبکه PBH در طی پیاده سازی سیستم تشخیص نفوذ پیشنهادی استخراج شده است . هدف بررسی و مقایسه کارایی و هزینه دو شبکه عصبی BP و PBH نشان داد که شبکه PBH با داشتن تعداد نورون های مخفی کمتر دارای نرخ اعلان خطای پایینتری می باشد و در نتیجه کارایی بالاتری نسبت به شبکه BP دارد و همچنین با کاهش تعداد نورون های مخفی در شبکه PBH هزینه محاسبات نیز در این شبکه کاهش می یابد .

در " ساخت سیستم خبره برای تشخیص نفوذ در شبکه های کامپیوتری " مدلی برای ساخت سیستم های تشخیص نفوذ پیشنهاد شده است که بر اساس آن امکان شناسایی خودکار الگوهای نفوذ ناشناخته وجود دارد در این مدل ابتدا نماهای رفتار عادی در سطح شبکه ایجاد می شود , سپس هر رفتار جدید که از نماهای رفتار عادی انحراف داشته باشد و با الگوهای نفوذ شناخته شده مطابقت نکند , به عنوان یک نفوذ جدید تشخیص داده می شود . با استفاده از روش های یادگیری از روی نمونه ها , الگوهای این نفوذ های جدید شناسایی و به اطلاع مسئول امنیتی سیستم رسانده می شود . مسئول امنیتی هم می تواند الگوهای نفوذ به دست آمده را پس از بررسی به پایگاه الگوهای نفوذ شناخته شده قبلی , اضافه کند . در ادامه نمونه مدل پیشنهادی پیاده سازی شده است . در این نمونه سعی شده است تا الگوهای نفوذ ناشناخته در سطح ترافیک شبکه شناسایی شود . در نمونه پیاده سازی شده , برای ایجاد نماهای ترافیک عادی و شناسایی الگوهای نفوذ ناشناخته از ترافیک شبکه , از ابزارهای یادگیری قانون $C_{4.5}$ و RIPPER استفاده شده است .

در " طراحی و پیاده سازی یک سیستم تشخیص نفوذ با استفاده از سیستم های چند عامله " نشان می دهد که عامل های تشخیص دهنده می توانند به صورت توزیع شده و کاملا مستقل از هم اجرا شده و با همکاری و ارتباط با یکدیگر یک سیستم تشخیص نفوذ توزیع شده تشکیل دهند که هیچ نقطه منفرد شکستی نداشته باشد . در ساختار ارائه شده , هیچ محل پردازش مرکزی وجود نداشته و تمامی عامل ها داده های محیا شده برای آن ها به صورت مستقل پردازش کرده و هر فعالیت مشکوک را برای دیگر عامل های شبکه باز می کنند . نرم افزار های کاربر و سیستم اجرا می شود بدون اینکه به صورتقابل ملاحظه ای منابع سیستم را مصرف کرده و یا باعث افزایش ترافیک شبکه هنگام یک حمله گردد.

در " کشف نفوذ به کامپیوتر با استفاده از روش های محاسبه نرم "روش های تشخیص نفوذ به سیستم های کامپیوتری بررسی شده و دو راهکار در این زمینه ارائه شده است . هرردو روش ارائه شده از جمله روش های تشخیص ناهنجاری هستند . روش های تشخیص نا هنجاری این مزیت را نسبت به روش های تشخیص امضا دارند که با تغییر الگوی حملات که به سادگی امکان پذیر است , دچار خطا در تشخیص نمی شوند . راهکار اول تکنیکی بر پایه قوانین فازی برای تشخیص نفوذ ارائه می دهد , این راهکار از مزایای الگوریتم های ژنتیکی در مرحله تولید قوانین استفاده می کند . در این راه حل قوانین به صورت فازی بیان شده اند زیرا مرز بین فعالیت نرمال و غیر نرمال را نمی توان به خوبی بیان کرد که این باعث آلارم غلط در بسیاری از سیستم های تشخیص ناهنجاری می شود . به هر حال با استفاده از منطق فازی باعث ایجاد قابلیت تفسیر قوانین به کمک مفاهیم زبانی می شود . از طرف دیگر می توان نظرات افراد خبره را به راه حل وارد کرد . در این راهکار با وارد شدن نمونه جدید تهاجم لازم نیست مرحله آموزش از ابتدا شروع شود بلکه می توان از قوانین قبلی در نسل اولیه الگوریتم ژنتیکی استفاده کرد که سرعت همگرایی را افزایش می دهد . راهکار دوم ارائه شده یک روش آماری بر پایه تکنیک نزدیک ترین همسایه است این روش از تعداد کمی ویژگی متعامد که در مرحله پیش پردازش به دست آمده اند برای تشخیص نفوذ استفاده می کند . تعداد کم ویژگی باعث سرعت بیشتر این روش نسبت به روش های مشابه می شود به علاوه با استفاده از مجموعه ای از بهترین ویژگی ها به یک سیستم کلاس بندی قوی می توان رسید . زمان آموزش این روش نیز در مقایسه با روش هایی مانند شبکه عصبی فوق العاده کوتاه است . سیستم تشخیص یا بر اساس اطلاعات ذخیره شده فعالیت ها در سیستم نهایی یا ترافیک شبکه کار می کنند . در این تحقیق از اطلاعات خام IP/TCP مربوط به داده های تشخیص نفوذ Darpa استفاده شده است . در داده ها ۴۱ ویژگی برای هر نمونه وجود دارد و یک مساله دو کلاسی (یا پنج کلاسی) است . با استفاده از این دو راهکار سیستم های کلاس بندی مناسبی ایجاد شده است که بسته به نوع کاربرد می توان هر یک را به کار برد .

در " تشخیص نفوذ با رویکرد گذار حالت " روشی ارائه می شود که در آن علاوه بر فراخوانی های سیستمی انجام شده توسط یک برنامه , فراخوانی های تابعی درون برنامه نیز در نظر گرفته می شود . بدین ترتیب تشخیص نفوذ در سیستم را می توان در دوسطح فراخوانی تابعی و سیستمی انجام داد . در این سیستم ابتدا منطق برنامه از روی ضوابط طراحی آن به دست آورده شده و به صورت دیاگرام گذار حالت نشان داده می شود . بررسی انطباق فراخوانی های تابعی و نیز فراخوانی های سیستمی با منطق برنامه به دو صورت زمان واقعی و غیر پیوسته انجام می شود و در صورت وجود اختلاف رخداد یک حالت غیر عادی به اطلاع مسئول سیستم می رسد . مسئول امنیت با توجه به سیستم های امنیتی و تجربیات خود می تواند نسبت به قطع اجرای برنامه مورد نظر اقدام کند .

در " سیستم تشخیص نفوذ مبتنی بر یکپارچگی بسته اطلاعاتی TCP "روش جدیدی برای مشخص کردن حملات قطعه قطعه کردن بسته اطلاعاتی TCP ارائه شده ات , به طوریکه برای تشخیص حمله نیازی به بازسازی کامل بسته اطلاعاتی نمی باشد و در نتیجه زمان لازم برای چک کردن بسته اطلاعاتی کاهش می یابد , در این روش برای مشخص شدن حمله فقط به فیلد های خاصی در هر بسته نیاز است .

بررسی کارهای انجام شده و مقالات خارجی

یک رساله به نام ADAM "بررسی عملکرد داده کاوی در تشخیص نفوذ" به بحث در مورد شیوه های داده کاوی در تشخیص نفوذ می پردازد.ADAM یک تشخیص دهنده نفوذ است که ساخته شده تا با کاربرد تکنیک های داده کاوی , نفوذ ها کشف شوند . این سیستم ابتدا داده های آموزشی که آزاد از حملات هستند را جذب میکند , سپس با کاربرد الگوریتم حملات , رفتار ناشناخته و هشدار های غلط را گروه بندی میکند. این آشکار سازها با کاربرد قواعد مربوط علم و دانش در مورد این داده ها را ذخیره سازی میکند . در آینده , تلاش میشود ضرورت های داده های آموزشی , که به سختی بدست می آیند کاهش یابند همچنین تلاش میشود نتایج یک شبکه سنسور ترکیب شود . ADAM چند قابلیت مهم دارد که نویسندگان آنها را شرح می دهند:

- طبقه بندی یک مورد به عنوان یک حمله شناخته شده
- طبقه بندی یک مورد به عنوان یک رویداد طبیعی
- طبقه بندی یک مورد به عنوان یک حمله ناشناخته
- تطبیق داده های ردیاب نظارت بر قوانینی که خود ADAM بوجود می اورد.

ADAM در آغاز کار , ابتدا یک مجموعه رفتار طبیعی را داده کاوی هایی که معلوم است آزاد از حملات هستند را ذخیره سازی میکند , سپس با کاربرد یک روش بر خط ارتباطات آینده را با مجموعه اطلاعات نرمال مقایسه میکند . آنهایی که جفت و منطبق نیستند بعدا بررسی می شوند . پس از آن ADAM از یک مامور طبقه بندی استفاده میکند و داده های مشکوک را در یکی از سه گروه زیر قرار میدهد : هشدار غلط , حمله ناشناخته یا حمله شناخته . بعد از تست نسبت به شش تکنیک دیگر , معلوم شد از کل مجموع ارزیابی های درست در رده دوم است و در موقع محاسبه درصد حملاتی که کشف میکند در رده سوم قرار میگیرد . این حاکی از این است که سرعت منفی غلط آن نسبت به سرعت مثبت غلط بالاتر است . درحالیکه این مساله ممکن است باعث شود حملات را از دست بدهد, اما تعداد اخطارهای مثبت و غلط منتج شده را کاهش می دهد. در , نویسندگان با کاربرد یک شبکه نوروفازی یک روش تشخیص نفوذ ارائه می دهند . این نوع الگوریتم یادگیری شبکه های مصنوعی و سیستم های استنتاجی فازی همچنین الگوریتم های تکاملی را ترکیب می کند . انها یک الگوریتمی ابداع می کنند که از قوانین فازی استفاده می کند و نورون های جدیدی برای این کار خلق می کنند . محققان از Snort استفاده می کنند و برای آموزش الگوریتم , داده جمع آوری می کنند . آنها تکنیک خود را با یک سیستم عصبی غیر افزونی مقایسه می کنند . طبقه بندی قیمت دو الگوریتم مشابه است و هردو برای انواع حملات مقایسه شده یک دقت بسیار بالایی داشته اند . آنها نشان می دهند که گذشته از این با کاربرد ۴۰ درصد متغیر ورودی کمتر نتایج معتبری داشتند . ADMIT یک سیستم تشخیص نفوذ مبتنی بر رفتار غیر عادی است که با دسته بندی داده های خود بین کاربر نرمال و غیر نرمال کامپیوتر تمایز ایجاد میکند . این سیستم مبتنی بر میزبان است برعکس اینکه مبتنی بر شبکه باشد.مسائل امنیتی که این سیستم تشخیص نفوذ کنترل میکند شامل تشخیص رفتار غیر عادی است , بعداز اینکه مزاحم بایک ترمینال بی مراقب , حدس زدن یک پسورد یا به عنوان یک کاربر مجاز این سیستم دسترسی پیدا کرد.چند مزیت این سیستم اینست که آن مراکز دسته ها را به مدیر نشان میدهد , با این امید که داده هایی که مدیر باید کپی کند کاهش یابد علاوه بر این , نویسندگان میگویند که ADMIT نسبت به روش های دیگر به زمان آموزش کمتری نیاز دارد. همچنین سیستم آنها نسبت به سیستم دیگر با کاربرد مجموعه داده ی مشابه یک طبقه بندی درست تری از رفتار ارائه میدهد. این مقاله مفصل در مورد الگوریتم های کاربردی توضیح میدهد . همچنین در مورد مجموعه داده استفاده شده بحث می کند , که از رساله تی لین از دانشگاه پردو گرفته شده است . این مقاله نقل میکند که نرخ تشخیص به بزرگی ۸۵/۳ در صد و مثبت های غلط ۱۵/۳ در صد است . این مقاله از طرفی توضیح میدهد چگونه این نویسنده ها پارامترهای الگوریتم خود را تغییر داده اند و یک خلاصه در مورد تاثیر این تغییرات بر نتایج ارائه میدهند. در "تکنیک های هوش مصنوعی قابل کاربرد در تشخیص نفوذ" یک تکنیک برای تشخیص نفوذ با کاربرد شبکه های نوروفازی و منطق فازی پیشنهاد میکند.ضبط داده با کاربرد Snort انجام میشود.آنها یک معماری برای سیستم تشخیص نفوذ هوشمند پیشنهاد میکنند. کار آنها در مرحله مقدماتی است و نتایج آزمایش در این مقاله ارائه نمیشود. در " تشخیص نفوذ شبکه های بی سیم با کاربرد دسته بندی تکنیک ها با آنالیز خبره " یک شیوه بدون سرپرست برای تشخیص نفوذ ارائه میشود. در" یک شیوه اجرای یک سیستم تشخیص نفوذ شبکه ها با استفاده از الگوریتم های ژنتیکی " الگوریتم ژنتیکی به عنوان یک ابزار دیگر برای آنالیز رده های نظارت امنیتی معرفی میشود . این مقاله به شیوه ای میپردازد که بو سیله آن دو الگوریتم ژنتیک قوانین را ارزیابی میکند , درحالیکه برای کاهش سرعت اخطار غلط و افزایش سرعت تشخیص

نفوذ قوانین بیشتری ایجاد میکند و نتایج سرعت تشخیص با این حال در دسترس نیستند . در مقاله ای با عنوان " یک شیوه داده کاوی بار تشخیص نفوذ پایگاه داده " یک سیستم توصیف میشود که از داده کاوی طبق وابستگی داده در یک پایگاه داده استفاده میکند و تغییرات منطبق بر یک حمله را شناسایی میکند . در " داده کاوی برای کشف امضا در یک سیستم تشخیص نفوذ مبتنی بر شبکه " یک سیستم به نام sign sniffer اجرا میشود . این روش شیوه های داده کاوی و مبتنی بر قاعده را ترکیب میکند . نویسنده ها مدعی هستند یک شیوه پیشرفته داده کاوی برای امضاها ارائه میدهد . روش های داده کاوی برای ایجاد یک سیستم کشف امضا استفاده میشوند. در" کاربرد هوش مصنوعی در یک سیستم هیبرید تشخیص نفوذ ", تشخیص نفوذ با کاربرد شبکه های عصبی و منطق فازی بخث میشود. در " کاربرد یک شیوه داده کاوی های توزیع شده در ت شخیص نفوذ شبکه " , نوی سنده ها نقل میکنند که جمع آوری و آنالیز داده از چند میزبان ممکن ا ست غیر ممکن با شد . بنابراین , به جای تلاش به این کارها آنها یک فایل سوابق شبکه با آنالیز داده های توزیع شده ایجاد میکنند و این فایل سوابق گذ شته , اطلاعات در مورد شبکه را به جای اطلاعات در مورد نفوذ های فردی ثبت میکنند. در سیستم توصیف شده آنها تنها محل داده در یک کامپیوتر (نه خود آگاه) باید کامپایل شـــود را به یک درخت تصـــمیم گیری منتقل می کنند . آنها می توانند همچنین انتقال شاخص ها به محل چنین داده ها در شبکه را فشرده سازی کنند. همچنین تفاوت بین شبکه های مصنوعی و شبکه عصبی هیبرید آن ها را ارزیابی می کند . این تفاوت ها تا حدودی کوچک هستند , که ممکن است نشان دهند یک شبکه عصبی در صورتی اجرا می شود که اهمیت آماری نتایج در نظر گرفته شوند . البته , شبکه عصبی فازی سریع تر اجرا می کند .

جدول ۱-۱ مقایسه بین ANN,EFuNN

	در صد ی که درست تشخیص داه شده	
	EFuNN	*ANN*
Normal	٪۹۹/ ۵۶	٪۹۹/۵۷
Probe	٪۹۹/۸۸	٪۹۴/۶۲
Dos	٪۹۸/۹۹	٪۹۸/ ۹
U2R	٪۶۵	٪۵۹/۰۰

طبق این جدول می توان استنباط کرد گروه U2R پایین ترین درصد ارتباطات که درست تشخیص داده شده اند دارد . نویسندگان می گویند که EFuNN در این مرحله آموزش به چند ثانیه نیاز دارد در حالیکه ANN به چند دقیقه نیاز دارد . آن ها نتیجه می گیرند که زمان آموزش سریع , نتیجه کاهش تعداد خصوصیات است . همچنین , این نویسنده معتقد است که تعداد نمونه های آموزشی کمی به زمان آموزش سریع نسبت داده می شود البته این مقاله به مبادله های کاربرد یک تعداد خصوصیات متفاوت اشاره نمی کند . یک مقاله به بحث در مورد ADMIT IDS می پردازد از یک مجموعه داده استفاده می کند که از رساله تی لین از دانشگاه پردو مشتق شده است . آزمایشگاه لینکلن MIT چند مجموعه داده دارد که بخشی از " ارزیابی تشخیص نفوذ DARPA " هستند . اینها به مجموعه داده های ۱۹۹۸, ۱۹۹۹و ۲۰۰۰ تقسیم می شود . مجموعه داده ۱۹۹۸ محتوی هفت هفته داده آموزشی و دو هفته داده آزمایشی است . داده ی نفوذ DARPA 99 محتوی سه هفته داده آموزشی و دو هفته داده تستی است . داده نفوذ DARPA 2000 محتوی مجموعه های داده برای دو سناریو جایی که یک حمله کننده ی مبتدی بر ضد یک مدافع ساده یک حمله را اجرا میکند .

نتیجه گیری

به طور کلی سیستم های تشخیص نفوذ دارای نقاط ضعف نسبتاً زیادی در تشخیص حملات جدید و تشخیص رفتار غیر عادی شبکه هستند، از طرف دیگر امروزه برای تشخیص حملات روی شبکه های مهمی از جمله شبکه های بیسیم، نیاز به نرم افزارهای هوشمند تری می باشیم، زیرا که یک نفوذگر باهوش همیشه برای مخفی کردن حملاتش، راه های هوشمندانه ای را انتخاب می کند. مهاجمین ممکن است که از تکنیک های مخفی سازی استفاده کنند که بسیاری از سیستم های تشخیص نفوذ در حال حاضر توانایی شناسایی آن ها را ندارند. به طور

قطع تشخیص یک حمله کار بسیار مشکلی می باشد ویا اینکه پس از تشخیص حمله، امکان شناسایی نوع حمله و آنکه مهاجم چه کاری انجام می دهد دشوارتر است و در کل آنکه برای تشخیص و ارائه عملکرد مناسب نیاز به تکنیک های پیچیده تر و هوشمندانه تری داریم. بنابراین نیاز به رویکردی جدید در خصوص هوشمند سازی سیستم تشخیص نفوذ امری الزامی است. به طور کلی روش های متعددی برای هوشمند سازی این سیستم ها پیشنهاد شده و در حال تحقیق و توسعه است که از آن جمله می توان به استفاده از الگوریتم های ژنتیک، سیستم های خبره، منطق فازی و شبکه های عصبی اشاره نمود. که هر کدام دارای ویژگی های خاص بوده و استفاده از آن ها توانایی سیستم ا در برخورد با حملات جدید و رفتار غیر عادی نشان خواهد داد.در این پروژه یک الگوریتم و روش بهبود سیستم تشخیص نفوذ Snort با استفاده از یک پایگاه دانش ارائه شده که قابلیت Snort را در تشخیص غیر عادی رفتار شبکه و حملات جدید بالا ببرد. به این منظور دو نوع تکنیک و روش به منظور پیاده سازی این الگوریتم ارائه می شود که عبارتند از بکارگیری Nmap وبکارگیری مدل آماری که در این پایان نامه، با استفاده از تکنیک اول SPP-NMAP را به سیستم Snort جهت بهبود وضعیت آن اضافه می کنیم.

تقدیر و تشکر

این مقاله از پایان نامه دوره کارشناسی ارشد رشته کامپیوتر مصوب و دفاع شده در دانشگاه آزاد واحد بروجرد استخراج شده است. نویسنده بر خود لازم میدانند مراتب تقدیر و تشکر صمیمانه خود را از آقای دکتر افشین رضاخانی استاد دانشگاه آزاد واحد بروجرد، که بنده را در انجام و ارتقاء کیفی این پژوهش یاری دادند، اعلام نماید.

منابع

S. Chavan, K. Shah, N. Dave, S. Mukherjee, A. Abraham, and S. Sanyal, "Adaptive neuro-fuzzy intrusiondetection systems," itcc, vol. 01, p. 70, 2004.
S. B. Idris, N.B., "Artificial intelligence techniques applied to intrusion detection," in INDICON, 2005 Annual IEEE, pp. 52–55–11–13, December 2005.
Y. Hu and B. Panda, "A data mining approach for database intrusion detection," in SAC '04: Proceedings of the 2004 ACM symposium on Applied computing, (New York, NY, USA), pp. 711–716, ACM Press,2004.
http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html,2007 Studies, 27(3):221–234
Snort User Manual Network Intrusion Detection_system. http://www.snort.org
Yang Xiang-Rong,S.Jun-Yi,"Implementation Of Sequence Patterns Mining in Network Intrusion System",IEEE 2001
http://www.cert.org/
Srinivas Mukkamala,Andrew H.Sung,Ajith Abraham,"Intrusion detection using ensemble of intelligent Paradism",New Mexico tech,Journal of Network and computer application,Elsevier,Janurary 2004
Yoann Vandoorselaere, Laurent Oudot, Prelude Intrusion Detection System,
http://www.prelude-ids.com
Prelude User Manual. http://www.prelude-ids.com
The Snort Core Team. "The Snort FAQ", http://www.snort.org. 2005.
http://www.snort.org/docs/,SnortTMUsers Manual 2.8.1
M. Roesch. Writing Snort Rules: How To write Snort rules and keep your sanity. http://www.snort.org.
Mohd Faizal Abdollah, Asrul Hadi Yaacob," Revealing the Influence of Feature Selection for Fast Attack Detection", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.8, August 2008.
Jalili R., Fatemeh IM., Morteza A., Hamid RS. "Detection of Distributed Denial of Service Attacks Using Statistical Pre-processor and Unsupervised Neural Network.", ISPEC, Springer-Verlag Berlin Heidelberg, 2005.
Anazida Z., Aizaini MM., Mariyam S. (2006). Feature_ Selection Using Rough Set in Intrusion Detection. In_ Proceeding of the IEEE Region 10 Conference TENCON_ 2006, IEEE, 2006