دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

ارائه یک راهکار جدید مبتنی بر داده‌کاوی جهت همبسته‌سازی هشدارهای تشخیص نفوذ

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر-هوش مصنوعی

محمد ایمانیان بیدگلی

استاد راهنما

دکتر عبدالرضا میرزایی

1392


بسم الله
الرحمن
الرحيم

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

ارائه یک راهکار جدید مبتنی بر داده‌کاوی جهت همبسته‌سازی هشدارهای تشخیص نفوذ

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر-هوش مصنوعی

محمد ایمانیان بیدگلی

استاد راهنما

دکتر عبدالرضا میرزایی

1392

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر-هوش مصنوعی

تحت عنوان

ارائه یک راهکار جدید مبتنی بر داده‌کاوی جهت همبسته‌سازی هشدارهای تشخیص نفوذ

در تاریخ 92/10/2 توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

1- استاد راهنمای پایان نامه .....دکتر عبدالرضا میرزایی

2- استاد مشاور پایان نامه .....دکتر مهدی برنجکوب

3- استاد داور.....دکتر علی فانیان

4- استاد داور.....دکتر مهران صفایانی

5- سرپرست تحصیلات تکمیلی دانشکده ..... دکتر سید محمد علی خسروی فرد

تشکر و قدردانی

خدا را سپاس که لطف بی پایانش همیشه شامل حال من بوده و بار دیگر در سایه‌ی لطف بی دریغش توانستم یکی از مراحل زندگی ام را به انجام برسانم.

مطمئناً انجام این پایان نامه بدون راهنمایی ها، پشتیبانی ها و تشویق های کسانی که مرا در طول این مسیر یاری کردند، امکان پذیر نبود. در ابتدا از راهنمایی و حمایت استاد راهنمای گرانقدرم جناب دکتر میرزایی تشکر می‌نمایم که همواره در طول انجام این پایان نامه، راهنما و مشوق من بوده اند. از جناب دکتر برنجکوب به دلیل مشاوره های بی دریغشان کمال تشکر را دارم. ایشان با فراهم نمودن فرصت پژوهشی مناسب در شرکت پیام پرداز نقش به سزایی در راستای شکل‌گیری و جهت دهی این پایان نامه داشتند. همچنین لازم می‌دانم از دوستان و همکاران خوبم در شرکت پیام‌پرداز بخصوص جناب مهندس احمدرضا نوروزی تشکر ویژه ای داشته باشم چرا که مدت همکاری با این عزیزان و استفاده از مشاوره ها وتجربیات ایشان نقش مؤثری در کاربردی شدن این پایان نامه ایفا نمود.

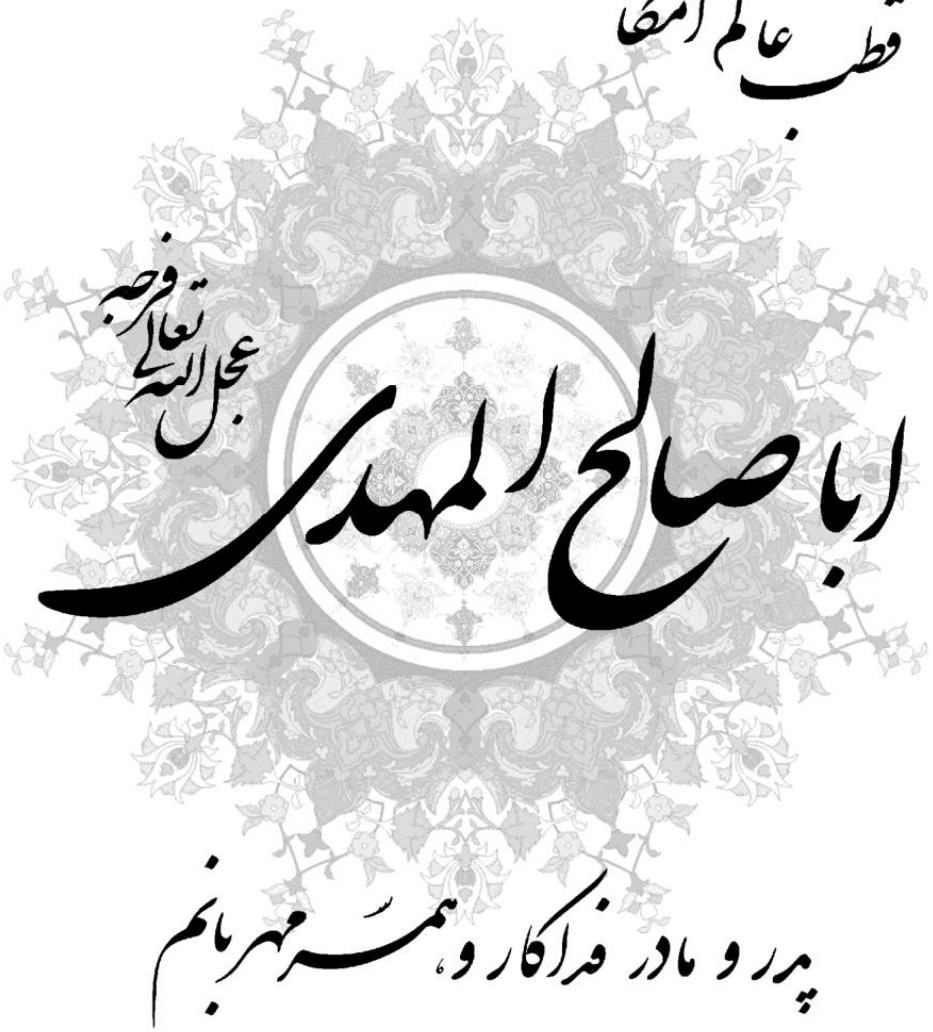
لازم میدانم از جناب دکتر فانیان به خاطر مشاوره های بی دریغ و همچنین داوری این پایان نامه و دکتر صفایانی به خاطر داوری این پایان نامه کمال تشکر را داشته باشم.

بدون شک پشتیبانی ها، حمایت ها و تشویق های همسرم و تحمل صبورانه سختی های زندگی دانشجویی ، یکی عوامل موفقیت من بوده است که هر چند جبران پذیر نیست ولی بدین وسیله از او تشکر و قدردانی می نمایم. نقش زحمت ها وخون دلهای بی چشم داشت پدر و مادر در هیچ یک از مراحل زندگی انسان را نمی توان نادیده گرفت. هر چند جبران پذیر نیست اما از پدر و مادر عزیزم بخاطر لطف بی دریغشان قدردانی می‌نمایم.

محمد ایمانیان بیدگلی ، زمستان 1392شمسی

تقدیم به

قطب عالم امکان



پدر و مادر فداکار و همسر مهربانم

فهرست

چکیده

با روند رو به رشد استفاده از شبکه های کامپیوتری به خصوص اینترنت و مهارت رو به رشد کاربران و مهاجمان این شبکه ها و وجود نقاط آسیب پذیری مختلف در نرم افزارها، ایمن سازی سیستم ها و شبکه های کامپیوتری ، نسبت به گذشته از اهمیت بیشتری بر خوردار شده است. یکی از ابزارهای مهم در تشخیص حملات، سیستم‌های تشخیص نفوذ هستند. در حال حاضر مهمترین چالش در استفاده از این ابزار، حجم بالای هشدارهای تولیدی توسط آن‌هاست که عملاً امکان رسیدگی به هشدارها را از بین می‌برد. به همین منظور تحقیقات گسترده‌ای در زمینه‌ی گام‌های پس‌پردازش و همبسته‌سازی هشدارهای تشخیص نفوذ صورت گرفته است. به طور کلی روش‌های همبسته‌سازی هشدار به دو دسته روش‌های مبتنی بر دانش و روش‌های استنتاجی تقسیم می‌شوند. روش‌های استنتاجی دسته روش‌هایی هستند که از تحلیل‌های آماری و تکنیک‌های هوش مصنوعی برای همبسته‌سازی هشدارها، بهره می‌برند. پژوهش پیش‌رو تلاشی است برای ارائه یک راهکار کارآمد و موثر، مبتنی بر تکنیک‌های داده‌کاوی و تحلیل‌های آماری در راستای همبسته‌سازی هشدارهای تشخیص نفوذ. در این تحقیق سعی شده با مطالعه‌ی میدانی هشدارهای تشخیص نفوذ نیازمندی‌های اصلی یک سیستم همبسته‌ساز، شناسایی و با کمک الگوریتم‌های کارآمد پیاده‌سازی شود. روش ارائه شده سعی دارد تا الگوهای رخداد هشدارها را کشف کند و آنها را در قالب قوانین همبسته‌سازی در اختیار مدیر سیستم بگذارد. در این روش با محاسبه میزان رخداد الگوهای مختلف هر جفت هشدار و همچنین با اعمال مشخصه‌های تشابه دو هشدار، اقدام به محاسبه‌ی میزان همبستگی هر جفت هشدار می‌کنیم. با اعمال مشخصه‌های تشابه از همبسته شدن الگوهای تصادفی جلوگیری می‌شود. بعد از محاسبه میزان هر جفت هشدار، در یک ساختار گام به گام عمل همبسته‌سازی هشدارها را انجام می‌دهیم. هر جفت هشدار همبسته شده در قالب یک هشدار جدید شناخته شده و در گام‌های بعدی الگوریتم، همبستگی این هشدارهای جدید با سایر هشدارها کشف می‌شود. این کار به صورت بازگشتی تا استخراج تمامی گام‌های حمله ادامه پیدا می‌کند. از جمله ویژگیهای این روش می‌توان به استفاده‌ی همزمان از پایگاه دانش زمینه ای و دانش مستخرج از هم‌رخدادی هشدارها، عدم استفاده از پنجره زمانی و در نتیجه امکان تشخیص حملات آهسته، عدم نیاز به آموزش، تشخیص انواع حملات یک به چند و چند به یک و امکان کشف الگوهای منظم تولید شده توسط بدافزارها اشاره کرد. برای سنجش کارایی این الگوریتم از مجموعه داده‌ی دارپا 2000 استفاده شده است و این روش با دو روش مرجع مشابه، مقایسه شده است. نتایج آزمایشات انجام شده، گواهی بر این مدعا است که روش مذکور توانایی رقابت با بهترین پژوهش‌های صورت گرفته در این زمینه، حتی روش‌های دانش پایه را دارا است.

کلمات کلیدی: 1- همبسته‌سازی 2- هشدار 3- تشخیص نفوذ 4- داده‌کاوی

فصل اول
مقدمه

1-1 مقدمه

با روند رو به رشد استفاده از شبکه های کامپیوتری به خصوص اینترنت و مهارت رو به رشد کاربران و مهاجمان این شبکه ها و وجود نقاط آسیب پذیری مختلف در نرم افزارها، ایمن سازی سیستم ها و شبکه های کامپیوتری ، نسبت به گذشته از اهمیت بیشتری بر خوردار شده است. تامین امنیت در هر سیستم یا شبکه کامپیوتری در واقع به معنای سه بعد اساسی محرمانگی، جامعیت و دسترس پذیری در آن می باشد که می توان به دو صورت، یکی از طریق پیشگیری امنیتی و دیگری از طریق تشخیص تخطی از سیاست‌های امنیتی انجام پذیرد. اکثر تحقیقاتی که تاکنون در زمینه امنیت کامپیوتر صورت پذیرفته است، تمرکزشان بر روی تامین امنیت با استفاده از روش های پیشگیرانه ای همچون استفاده از مکانیزم های هویت شناسی و اعتبارسنجی، کنترل دسترسی، رمزنگاری و حفاظ(دیواره ی آتش) بوده است. در حالی که به غیر از پیشگیری باید درپی درمان نیز بود. لذا تحقیق و بررسی بر روی سیستم های غیر پیشگیرانه همچون سیستم های تشخیص نفوذ که وظیفه ی شان تشخیص حمله و رفتارهای ناهنجار در سیستم ها و شبکه های کامپیوتری می باشد، نیز از اهمیت و جایگاه خاصی برخوردار است.

سیستم های تشخیص نفوذ[1](IDS) یکی از مهمترین ابزارهای امنیتی در شبکه های کامپیوتری هستند. تشخیص نفوذ فرآیند نظارت بر وقایع رخ داده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاست های امنیتی است. سیستم تشخیص نفوذ اینگونه نیز تعریف شده است «نرم افزاری با قابلیت تشخیص، آشکارسازی و پاسخ به فعالیت‌های غیرمجاز یا غیر عادی در رابطه با سیستم.»

[1] Intrusion Detection System (IDS)

سیستمهای تشخیص نفوذ بر مبنای نحوه تشخیص به دو دسته اصلی تقسیم می شوند:

- سیستمهای تشخیص سوء[1] استفاده
- سیستمهای تشخیص ناهنجاری[2].

سیستم های تشخیص سوء استفاده، پایگاه دانشی از الگوی[3] حملات دارند و چنانچه ترافیک شبکه با این الگو مطابقت داشته باشد، آن ترافیک را حمله، تشخیص می دهند. سیستمهای تشخیص سوء استفاده از محبوبیت زیادی برخوردار هستند زیرا به سادگی گسترش می یابند، دقت بالایی دارند و منابع کمتری مصرف می‌کنند.

ولی این سیستم ها دارای نقاط ضعفی نیز هستند:

- توصیف حملات معمولا خیلی سطح پایین بوده و بنابراین تعیین و تفسیر آنها دشوار است.
- برای هر حمله و هر گونه‌ی تغییر یافته از آن نیاز به اضافه کردن یک الگوی جداگانه به پایگاه دانش است که این امر باعث بالا رفتن اندازه پایگاه دانش می شود.
- هرچه الگوی حملات خاص تر باشد نرخ مثبت نادرست کمتر خواهد شد. ولی اگر الگوی حملات خیلی خاص باشد آنگاه مهاجم می تواند با ایجاد کمی تغییر در حمله مانع از کشف آن شود.

سیستمهای تشخیص ناهنجاری بر این فرض استوارند که هر فعالیت ناهنجار یک فعالیت بدخواهانه است. بنابراین ابتدا یک مدل از رفتارهای هنجار ایجاد می‌شود و سپس هر رفتاری که با آن مغایرت داشت به عنوان ناهنجاری شناخته می-شود. مزیت اصلی این گونه سیستم‌ها، این است که امکان تشخیص حملات ناشناخته را دارند، ولی به علت نرخ مثبت نادرست بالایی که دارند دقتشان بسیار پایین است. برخی از این سیستم‌های تشخیص ناهنجاری از تکنیک‌های یادگیری ماشین برای مشخص کردن پارامترهای رفتار هنجار سیستم استفاده می‌کنند، که این گونه سیستم‌ها معمولا با مشکلات زیر روبرو هستند:

- زمان زیادی برای یادگیری رفتارهای هنجار لازم است.
- رفتارها ممکن است در طول زمان تغییر کنند و نیاز به آموزش دوباره وجود دارد.
- اگر داده‌های یادگیری شامل حمله باشد، آنگاه ممکن است رفتارهای بدخواهانه به اشتباه، هنجار تشخیص داده شوند.
- امکان اجرای یک حمله به طوری که در حد و مرز رفتارهای هنجار قرار بگیرد وجود دارد.

علاوه بر دو دسته فوق، گروه دیگری از سیستم های تشخیص نفوذ هم وجود دارد که برخی آن را گونه ای از سیستم های تشخیص ناهنجاری می دانند و برخی دیگر آن را به عنوان دسته سوم سیستم های تشخیص نفوذ می‌دانند. این سیستم‌های تشخیص نفوذ، سیستم های تشخیص نفوذ مبتنی بر مشخصه[4] نام دارند که با ترکیب نقاط قوت سیستم های

---

[1] Misuse detection system
[2] Anomaly Detection System
[3] Signature
[4] Specification Based IDS

تشخیص سوء استفاده و تشخیص ناهنجاری به وجود آمده اند. در این سیستم ها، ویژگی های رفتاری برنامه های مجاز به صورت دستی بیان می‌شود. بنابراین این سیستم ها در هنگام مواجهه با رفتار غیر عادی(ولی مجاز) برنامه ها هشدار نادرست صادر نمی‌کنند و نرخ مثبت نادرست آنها قابل مقایسه با نرخ مثبت نادرست سیستم های تشخیص سوء استفاده است. این سیستم های تشخیص نفوذ با اشتقاق ویژگی های مجموعه ای از برنامه های مجاز داده شده، سایر برنامه های مجاز را می شناسند و امکان تشخیص حملات ناشناخته را نیز دارند.

سیستمهای تشخیص نفوذ از لحاظ دامنه عملیاتی نیز به دو دسته مبتنی بر میزبان و مبتنی بر شبکه تقسیم می شوند. سیستمهای مبتنی بر میزبان، حملات محلی یک میزبان را با استفاده از اطلاعات سیستم عامل یا برنامه‌های کاربردی تشخیص می‌دهند. از سوی دیگر، سیستمهای مبتنی بر شبکه حملات را با توجه به بسته‌های مبادله شده در شبکه تشخیص می‌دهند. اطلاعات تشخیص داده شده توسط سیستمهای مبتنی بر میزبان و سیستمهای مبتنی بر شبکه، مکمل یکدیگر هستند. اطلاعاتی نظیر پردازه و کاربر توسط سیستمهای مبتنی بر میزبان و اطلاعاتی نظیر مبدا، مقصد و پروتکل توسط سیستمهای مبتنی بر شبکه تشخیص داده می‌شوند.

هر دسته از این سیستم های تشخیص نفوذ نقاط ضعفی دارند و از این رو گاهی چند حسگر با روش های تشخیص متفاوت را در سیستم قرار می دهند تا عیوب یکدیگر را رفع کنند و نتایج بهتری ارائه کنند. به طورکلی دو یا چند IDS ممکن است برای اهداف زیر با یکدیگر همکاری کنند:

- تحلیل هشدارهای صادر شده یکدیگر: این حالت برای مواردی که سیستم های تشخیص نفوذ از روشهای تشخیص مختلف استفاده می‌کنند مناسب است؛ نظیر حالتی که یک سیستم تشخیص ناهنجاری در کنار یک سیستم تشخیص سوء استفاده، قرار می گیرد.
- تکمیل پوشش: به طور مثال دو IDS ممکن است هر دو مبتنی بر میزبان باشند و روی دو میزبان مختلف بوده، ولی هر دو درگیر یک حمله باشند. همکاری این دو باعث می‌شود اطلاعات جامع‌تری در مورد حمله به دست آید.
- تقویت هشدارهای یکدیگر و پایین آوردن نرخ مثبت نادرست: با مقایسه هشدارهای چند IDS مختلف امکان کاهش خطای مثبت نادرست وجود دارد.

2-1 مشکلات سیستم‌های تشخیص نفوذ

سیستم‌های تشخیص نفوذ عملاً دارای مشکلات عدیده‌ای هستند. یک طرف مبارزه در سیستم تشخیص نفوذ، هوش انسانی و یک نفوذگر حرفه‌ای است که در لباس میش ظاهر شده و مانند گرگ عمل می‌کند. بنابراین در طرف دیگر مبارزه نیز باید رفتاری هوشمندانه داشت. عملاً در اغلب سیستم‌های تشخیص نفوذ موجود، چنین سطحی قابل قبولی از هوشمندی وجود ندارد. مشکل اصلی سیستم‌های تشخیص نفوذ این است که حجم زیادی از هشدارهایی را تولید می کنند که ارتباطی به حملات واقعی ندارد. به دلائل مختلفی اعم از وجود الگوهای نادرست و یا غیر تخصصی منجر به

هشدارهای غلط می‌شود. این هشدارهای غلط موسوم به خطاهای مثبت کاذب[1] می‌باشند. همچنین بین هشدارهای تولید شده ارتباط منطقی وجود ندارد و فهم ارتباط واقعی در پشت این همه هشدار نیز غیر ممکن است. در این قسمت، مشکلات اصلی سیستم‌های تشخیص نفوذ را مورد بررسی قرار می‌دهیم.

1-2-1 هشدارهای سیل آسا

هشدارهای تولید شونده توسط سیستم‌های تشخیص نفوذ بسیار زیاد است و به شکلی سیل آسیا بر سر مدیر سیستم فرو می‌ریزد. سیستم‌های تشخیص نفوذ مبتنی بر شبکه هر بسته را جداگانه و مستقل بررسی می‌نماید و در بدترین حالت ممکن است کل ترافیک شبکه را به عنوان حمله گزارش دهد. مدیر سیستم نمی‌تواند حجم زیادی از هشدارهای مستقل از هم را بررسی و مدیریت نماید. بسیاری از این هشدارها تکراری و تعداد زیادی از آنها غلط هستند. به همین دلیل عملاً قابل استفاده برای مدیر نیستند. نادقیق بودن قوانین تشخیص حمله در سیستم‌های مبتنی بر الگو، دقیق نبودن تفاوت بین رفتارهای معمول و غیر معمول در سیستم‌های مبتنی بر ناهنجاری، باعث تولید هشدارهای غلط می‌گردد. البته لازم به ذکر است که هشدارهای غلط در سیستم‌های تشخیص نفوذ به معنای رخداد یک هشدار بدون وجود نشانه از رفتار بدخواهانه نیست. لفظ هشدارهای غلط، به هشدارهایی اطلاق می‌شود که هر چند نمایانگر وجود ترافیک منطبق با آن امضاء بوده است، اما به دلایل مختلف مانند عدم وجود آسیب‌پذیری متناسب و یا عدم دقت در تعریف الگو، آن ترافیک یک حمله نبوده است. از این رو هشدارهای مربوط به حملات واقعی که معمولا به ندرت رخ می‌دهند در میان هزاران هشدار غلط مخفی شده و قابل تفکیک نخواهند بود. در سیستم‌های تشخیص نفوذ مبتنی بر الگو قطعاً حملات ناشناخته تشخیص داده نمی‌شود و هشدارهای مربوط به آنها گم خواهد شد. علاوه بر آن به دلیل نادقیق بودن الگوهای حملات و یا مشکلات موجود در پیاده سازی سیستم‌های تشخیص نفوذ، برخی از هشدارها گم می‌شوند. در واقع علاوه بر تولید هشدارهای غلط، هشدارهای درست مربوط به حملات واقعی را نیز از دست می‌دهد.

2-2-1 نقص اطلاعات

مسئله دیگر سیستم‌های تشخیص نفوذ فعلی این است که هشدارهایی که ارائه می‌دهند اطلاعات کافی جهت اتخاذ یک تصمیم آگاهانه برای مدیریت حادثه در اختیار مدیران قرار نمی‌دهند. یکی از دلائل ناقص بودن اطلاعات این است که حسگرهای سیستم‌های تشخیص نفوذ تنها در یک حوزه عمل می‌کنند. یک سیستم تشخیص نفوذ مبتنی بر شبکه تنها بر روی ویژگیهای مبتنی بر شبکه مانند آدرس IP و شماره پورت عمل می‌نماید. بنابراین در رابطه با وضعیت امنیتی سیستم‌های میزبان تحت حفاظت خود، اطلاعات کمتری ارائه می‌نماید. به عنوان نمونه، از شناسه کاربر و یا شناسه فرآیندهایی که اتصالات شبکه را پاسخ می‌دهند بی اطلاع است. مشابه با آن، حسگرهای مبتنی بر میزبان نیز اطلاعات کمتری راجع به خصوصیات شبکه‌ای مربوط به یک حمله ارائه می‌نمایند. یک حسگر مبتنی بر میزبان که یک حمله سرریز بافر را گزارش می‌دهد ، معمولا آدرس حمله کننده را ارائه نمی‌کند زیرا در سطحی که کار می‌کند به این اطلاعات دسترسی ندارد. همچنین اولویت بندی معنادار غالباً در هشدارهای سیستم‌های تشخیص نفوذ وجود ندارد. در واقع هشدارها مستقل از هم هستند و ارتباط منطقی بین هشدارهای تولید شده ارائه نمی‌شود. به بیان دیگر هشدارها بسیار

[1] False Positive

سطح پایین هستند. این در حالی است که حملات واقعی از تعدادی گام تشکیل می‌شوند که با تکمیل گامها نفوذگر به منبع مورد نظر دسترسی پیدا می‌کند. با وجود مشکلات بیان شده در کنار حجم بسیار زیاد هشدارهایی که حسگرها تولید می‌کنند، ارائه یک تصویر سطح بالا از وضعیت امنیتی شبکه بسیار مشکل خواهد بود.

3-2-1 هشدارهای نامربوط

تعریف یک هشدار نامربوط این است که هشداری در مقابل یک حمله واقعی گزارش شده است اما به دلیل پیکربندی و یا نبود آسیب پذیری متناظر با آن بر روی سیستم مقصد، حمله‌ی صورت گرفته موفق نیست. مثلاً حمله‌ای که علیه سیستم عامل ویندوز وجود دارد، در مورد سیستمی گزارش شده است که سیستم عامل آن لینوکس است. علت این مشکل این است که حسگرهای تشخیص نفوذ اطلاع کافی در رابطه با میزبانهای تحت حفاظت خود ندارند. همچنین از موفق بودن حمله بر روی سیستم مقصد آگاهی ندارند. سیستم‌های تشخیص نفوذ مبتنی بر شبکه معمولاً تفاوتی بین حملات موفق و ناموفق قائل نمی‌شوند.

برخی از مشکلات سیستم‌های تشخیص نفوذ را در خود سیستم نمی‌توان حل کرد. در واقع قابلیتهای سیستم تشخیص نفوذ مبتنی بر میزبان را نمی‌توان به قابلیتهای سیستم تشخیص نفوذ مبتنی بر شبکه افزود. همچنین این دو سیستم از همه اتفاقات امنیتی که در شبکه رخ می‌دهد آگاهی کامل و دقیق نخواهند یافت و نیاز به اطلاعات دیگری به جز الگوهای حمله و آسیب پذیریها برای تشخیص حملات واقعی دارند. اما در کنار یکدیگر و با تلفیق اطلاعات سایر سرویسها، می‌توانند هشدارهای مناسبی را تولید نمایند تا وضعیت امنیتی شبکه و منابع آن به درستی ارائه شود. به عنوان مثال برای اینکه بدانیم یک هشدار تولید شده توسط سیستم تشخیص نفوذ، واقعا نمایانگر یک حمله است، لازم است که رابطه آن هشدار با هشدارهای قبل و بعد از آن به دقت بررسی شود و در صورتی که علائم دیگری از حمله دیده شد، آن هشدار و سایر هشدارهای مربوط به آن را به عنوان حمله گزارش کنیم. انجام این کار در قالب یک سیستم تشخیص نفوذ که می‌بایست به صورت بلادرنگ، حجم زیادی از ترافیک را زیر نظر داشته باشد، کار تقریبا غیر ممکنی می‌باشد.

یک راهکار برای حل این مشکلات حل نشدنی در سیستم‌های تشخیص نفوذ جمع آوری هشدارها در یک نقطه و تحلیل متمرکز آنها در مرکز عملیات امنیت[1] می‌باشد. بنابراین در کنار همه سیستم‌های تشخیص نفوذ و سایر سرویس‌های شبکه نیاز به یک تحلیلگر متمرکز برای کشف ارتباط بین انواع رخدادنماها می‌باشد تا تصویر دقیق و روشنی از وضعیت امنیتی شبکه ارائه گردد. یکی از مهمترین قسمت‌ها در مرکز عملیات امنیت، قسمت همبسته‌ساز می-باشد.

3-1 همبسته سازی هشدارهای تشخیص نفوذ

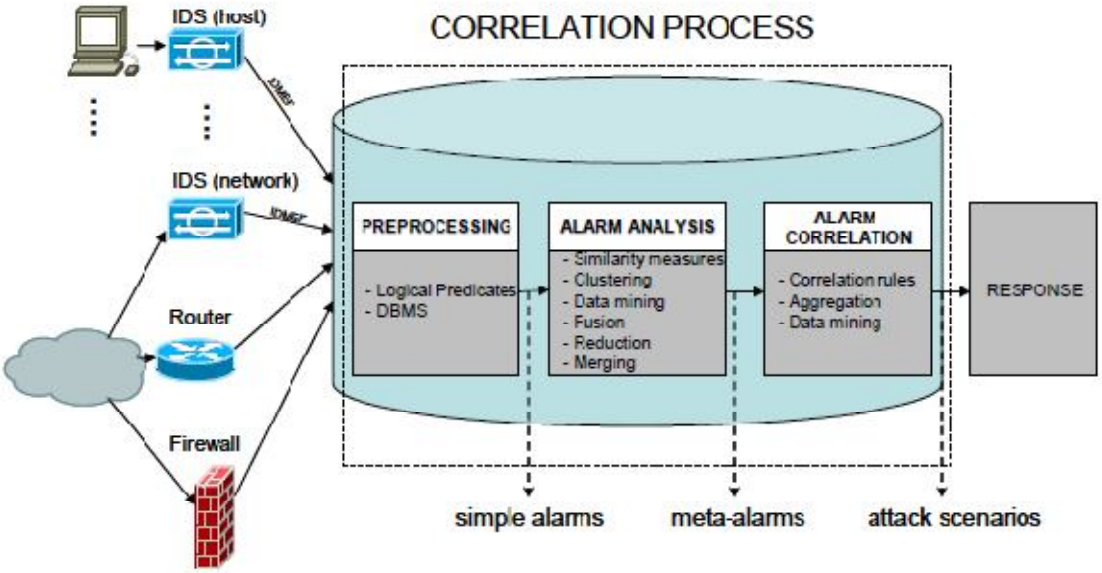
سیستم های تشخیص نفوذ به طور گسترده‌ای در شبکه ها به منظور افزایش امنیت به کار می روند، اما حجم بالای هشدارهای تولیدی این سیستم ها(به خصوص در حالت استفاده از چند نوع سیستم تشخیص نفوذ)، مدیریت این

[1] Security Operations Center (SOC)

هشدارها را دشوار می‌سازد و امکان تحلیل آنها و تصمیم گیری به موقع و مناسب در مقابل حملات را از مدیر امنیتی سیستم می گیرد.

سیستم‌های همبسته سازی برای رفع برخی از مشکلات سیستم‌های تشخیص نفوذ پیشنهاد شدند. سیستم‌های همبسته‌سازی هشدارها را از تعدادی از حسگرها دریافت کرده و برای تولید یک نگاه سطح بالا از وضعیت امنیتی جاری شبکه در یک فرآیند چندین مرحله‌ای پردازش می‌کنند. هدف اصلی یک سیستم تشخیص نفوذ کاهش تعداد هشدارهایی است که مدیر سیستم باید به طور دستی پردازش کند[1]. سیستم همبسته ساز هشدارهای غلط را شناسایی کرده، دور ریخته و هشدارهایی که مربوط به یک حادثه هستند را با هم گروه‌بندی کرده و اولویت بندی می‌نماید. همبسته سازی مورد نظر ما یک تحلیل صرفاً آماری بر روی هشدارها نیست، هرچند برخی از روش‌ها در این دسته قرار می‌گیرند. غالباً، همبسته‌سازها شامل ترکیبی از قوانین و پایگاه دانشی از اطلاعات راجع به شبکه مقصد است که بیان می‌کنند هشدارها چگونه باید با هم ارتباط داده شوند. یک حمله کننده ممکن است کارهای مختلفی اعم از پویش شبکه، اجرای حمله علیه یک سرویس، نصب برنامه‌های حمله مورد نظر تا رسیدن به مقصد مورد نظر انجام دهد. حسگرهای مختلف در شبکه گامهای مختلف حمله را گزارش خواهند داد.

از میان صدها هشداری که دریافت می‌شود تنها باید یک هشدار مربوط به یک حادثه به اطلاع مدیر سیستم برسد. پویشهای مختلف باید درون یک هشدار پویش سطح بالا گزارش گردد. هشدارهای مربوط به حملات ناموفق و هشدارهای حملات سطح بالا باید به عنوان یک حمله چند گامی با هم گروه بندی شوند. یک حمله چندگامی، یک ترتیبی از گامهای حمله است که یک حمله کننده انجام می‌دهد در حالی که هر گام حمله مستقل از موفق بودن یا موفق نبودن آن در گام قبلی است. یک هشدار سطح بالا باید ترتیب گامهای حمله را نشان دهد. گامهای حمله شامل پویش، شکست سیستم، نصب ابزار حمله و در نهایت پویش داخلی که از سیستم فاش شده شروع می‌شود تا یک حمله چندگامی دیگر را برای رسیدن به یک مقصد با ارزشتر یا طی کردن گام به گام مسیر حمله نهایی ترتیب دهد. همبسته سازی شامل تحلیل‌های مختلفی است که به صورت مرحله به مرحله بر روی هشدارها صورت گرفته و در هر مرحله از همبسته سازی هشدارها را کاهش داده تا به هشدارهای مناسب دست یابد. شکل 1 نمای کلی از یک فرایند همبسته سازی را نمایش می‌دهد.



شکل **1** نمای کلی از یک فرایند همبسته سازی

همبسته سازی هشدارها یک فرآیند چند مرحله‌ای است که هشدارهایی را که توسط یک یا چند IDS مختلف تولید شده است را گرفته و توصیف سطح بالاتری از فعالیت‌های بدخواهانه در شبکه را در اختیار مدیر امنیتی سیستم قرار می دهد.

علاوه بر حجم بالای هشدارها، می توان دلایل دیگری نیز برای اهمیت نیاز به همبسته سازی هشدارها برشمرد:

- نرخ بالای هشدارهای مثبت نادرست
- ایجاد امکان همکاری بین سیستم های تشخیص نفوذ
- ایجاد دید سطح بالاتری از رخدادهای بدخواهانه در شبکه برای مدیر امنیتی سیستم و کمک به تصمیم گیری درست و به موقع در مقابل حملات
- عدم تشخیص سناریوی حملات چندمرحله ای توسط سیستم های تشخیص نفوذ ساده

هشدارهایی که سیستم های تشخیص نفوذ تولید می کنند هشدارهایی سطح پایین هستند و چنانچه به صورت تک تک در نظر گرفته شوند تهدیدات واقعی سیستم را به درستی نشان نمی دهد. معمولا مهاجمین برای رسیدن به اهداف خود از حملات چند مرحله[1] ای استفاده می‌کنند. به این صورت که در ابتدا از یک یا چند آسیب پذیری در سیستم استفاده کرده و حمله خود را یک گام جلو می برند و سپس با بهره گیری از پیامدهای[2] این گام که پیش نیاز[3] گام بعدی است، گام بعدی حمله را اجرا می کنند و به این ترتیب حمله خود را گام به گام جلو می برند. سیستم های تشخیص نفوذ تنها

---

۱ Multi Step Attack
۲ Consequence
۳ Prerequisite

قادر به تولید هشدارهای سطح پایین برای هرکدام از گامهای حمله به صورت مجزا هستند و امکان تشخیص سناریوی حملات چند مرحله ای و ارتباط دادن هشدارهای یک حمله به یکدیگر را ندارند. بنابراین نیازمند ایجاد یک دید سطح بالاتر از وضعیت امنیتی سیستم هستیم. همبسته سازی هشدارها چنین تصویری را از سیستم با پردازش بر روی هشدارهای سیستم های تشخیص نفوذ تولید می کند.

4-1 اهداف پایان نامه

موضوع همبسته‌سازی هشدارهای تشخیص نفوذ بخصوص در سال‌های اخیر بسیار مورد توجه بوده است و روش‌های مختلفی برای پوشش جنبه‌های مختلف این مشکل ارائه شده است. عموم پژوهش‌های صورت گرفته سعی در این داشته اند که روشی جامع برای حل این مسئله ارائه کنند حال آنکه مسئله همبسته‌سازی هشدارهای تشخیص نفوذ ذاتاً مسئله‌ای پیچیده و دارای جنبه‌ها و ظرایف گوناگون است، به همین دلیل ارائه یک مدل جامع باید متناسب با مورد کاربرد و اهداف استفاده، انتخاب شود.

بهتر این است که پژوهشگران به جای ارائه یک مدل همه جانبه، سعی در ارتقاء جنبه های مختلف حل این مسئله داشته باشند و با ارائه یک تکنیک جدید و یا تکمیل یک جنبه از تکنیک‌های گذشته دست کاربران را برای انتخاب یک یا مجموعه‌ای از تکنیک‌های برتر با توجه به مورد استفاده، باز بگذارند.

بر این اساس در این تحقیق سعی خواهد شد تا با تکیه بر جنبه آماری بررسی هشدارها و تکنیک‌های داده‌کاوی، روشی جدید برای پیدا کردن الگوی رخداد هشدارها ارائه شود. مسلم است،آنچه می‌تواند به عنوان یک روش کاربردی مورد استفاده قرار گیرد، به کارگیری مجموعه ای از تکنیک‌هاست که هر یک جنبه‌های مختلفی از ابعاد این مسئله را پوشش می‌دهد و نهایتا این تجربه مدیر شبکه است که باید با مدیریت این تکنیک‌ها، سیستم را در سطح بازدهی لازم نگه دارد.

به عنوان مثال هر چند تکنیک‌های آماری و کاوش الگوهای پرتکرار می‌توانند در پیدا کردن الگوی کلی رخداد هشدارها و در نتیجه کاهش حجم هشدارها و یا الگوی حملاتی که توسط بدافزارها و یا ابزارهای مخصوص حمله تولید می‌شوند، موفق باشند اما این تکنیک‌ها، وقتی پای یک نفوذگر انسانی و هوشمند وسط باشد، ناکارآمد خواهند بود و هوش انسانی به راحتی می‌تواند آن‌ها را فریب دهد و دور بزند. موفق بودن این روش در تشخیص الگوی حملات بدافزارها و ابزارهای مخصوص حمله به دلیل این است که عموماً بدافزارها و ابزارهای حمله از آنجا که دارای الگوریتمی خاص هستند، از یک الگوی خاص و ثابت برای حمله استفاده می‌کنند و پیدا کردن این الگوها که دارای مشخصه‌های آماری ویژه ای هستند راحت‌تر است. به هر حال در این صورت هم، این تکنیک‌ها می‌توانند با کاهش و حذف سایر هشدارها و در نتیجه کم کردن تعداد هشدارها، مدیر شبکه یا سایر روش‌های بر مبنای دانش زمینه‌ای را در راستای رسیدگی به هشدارها یاری رساند و به طور غیر مستقیم باعث بالا رفتن بازدهی سیستم شود.

پس در این تحقیق سعی بر آن است که یک روش آماری مبتنی بر داده‌کاوی، با دیدگاه کارامدتر از پژوهش‌های قبلی ارائه شود و اشکالات موجود در روش‌های پیشین مبتنی بر تکنیک‌های آماری و داده‌کاوی به نحوی بر طرف شود.

5-1 ساختار پایان نامه

در فصل بعد مروری بر پژوهش‌های صورت گرفته در حوزه همبسته‌سازی هشدارهای تشخیص نفوذ خواهیم داشت. در فصل سوم به ارائه مدل پیشنهادی خواهیم پرداخت. در فصل چهارم به نتایج آزمایشات صورت گرفته و همچنین مقایسه این نتایج با سایر پژوهش‌ها اشاره خواهد شد و نهایتاً در فصل آخر به نتیجه‌گیری و ارائه پیشنهادات برای کارهای آینده خواهیم پرداخت.