دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

کشف بلادرنگ سناریوهای حمله از طریق همبسته‌سازی هشدارهای سیستم تشخیص نفوذ

پایان‌نامه کارشناسی ارشد هوش مصنوعی و رباتیک

زینب زالی

استاد راهنما

دکتر حسین سعیدی

بهار ۱۳۸۸

دانشگاه صنعتی اصفهان
دانشکده برق و کامپیوتر

پایان نامه کارشناسی ارشد رشته هوش مصنوعی و رباتیک خانم زینب زالی

تحت عنوان

کشف بلادرنگ سناریوهای حمله از طریق همبسته‌سازی هشدارهای سیستم تشخیص نفوذ

در تاریخ ۸۸/۲/۱۳ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای پایان‌نامه	دکتر حسین سعیدی
۲- استاد مشاور پایان‌نامه	دکتر سیدمسعودرضا هاشمی
۳- استاد داور	دکتر مهدی برنجکوب
۴- استاد داور	دکتر محمد دخیل‌علیان
سرپرست تحصیلات تکمیلی	دکتر علی محمد دوست حسینی

خدایا کسی در طی مراحل شکر تو به سر منزلی نمی رسد،

مگر آنکه باز چندان از احسانت بر او فراهم می آید،

که او را به شکری دیگر ملزم می سازد.

سپاس خدای را که ردای عقل بر قامت انسان برافراشت و منت بی پایان او را که مرا فرصت علم آموزی عطا فرمود.

سپاس خدای را که مرا آغوش پر مهر مادر و پشتوانه استوار پدر بخشید. پدر و مادری که گرمای وجودشان بهترین امید زیستنم بوده و هست. بی شک اگر راهنمایی ها و روشنگری هایشان چراغ راه من نبود، مرا یارای رسیدن به هیچ سر منزل موفقیتی نبود. سپاس خدای را که مرا خانواده ای گرم و دوست داشتنی بخشید. همراهی پیوسته آن ها را ارج می نهم.

سپاس خدای را که بر من منت نهاد به داشتن اساتید و معلمانی بزرگوار و ایثارگر. آنان که با چراغ دانششان مرا در سرزمین دانش بارور ساختند. از خداوند سعادتمندی همیشگیشان را خواستارم.

سپاس خدای را به خاطر تمام دوستان و هم نشینان باصفا و با محبت که در مسیر زندگیم مرا با ایشان آشنا ساخت. قدردان حضور و یاری همیشگیشان هستم.

از خداوند بزرگ می خواهم که فرصت علم آموزی را در این دنیا برایم تداوم بخشد. به من سعادت خدمت به مردمان را عطا فرماید، چنان که از علم و دانشی که به من مرحمت نموده است، جز در راه رضای او بهره نگیرم.

زینب زالی

اردیبهشت ۱۳۸۸

تقدیم به:

خوب خوب نازنینم، مادر مهربانم

و بهترین بهترینم، پدر عزیزم

به پاس زلال لطف بی کرانشان، موج دیدگان مهربانشان و

تمام امیدها، دلواپسی ها و آرزوهاشان

فهرست مطالب

عنوان | صفحه

چکیده

شبکه‌های کامپیوتری جزء اساسی جامعه اطلاعاتی امروزی محسوب می‌شوند. این شبکه‌ها معمولا به شبکه سراسری اینترنت متصل هستند. با توجه به این‌که امنیت از اهداف اولیه طراحی اینترنت نبوده است، در دهه‌های اخیر امن‌سازی این شبکه‌ها در برابر حملات از اهمیت بسیاری برخوردار شده است. امروزه جهت تأمین امنیت، سیستم‌ها و ابزارهای امنیتی متفاوتی از جمله سیستم‌های تشخیص نفوذ (IDS) در شبکه‌ها استفاده می‌شوند. IDSها با مشاهده هر نوع رویداد مشکوک که بیان‌گر استفاده غیرمجاز، سوء استفاده و یا آسیب رساندن به سیستم‌ها و شبکه‌های کامپیوتری باشد، هشدارهایی تولید می‌کنند. اما مشکلات زیادی در رابطه با این هشدارها وجود دارد، از جمله جریان سیل‌آسای هشدارها، وجود هشدارهای اشتباه، مفقودشدن بعضی از هشدارها و عدم تشخیص همبستگی بین هشدارهای همبسته. بنابراین برای استخراج اطلاعات مفید از هزاران هشدار تولیدشده توسط یک یا چند IDS، نیازمند تحلیل هشدارها هستیم. هر هشدار در IDS را می‌توان بیانگر یک حمله‌ی سطح پایین در نظر گرفت. همبسته‌سازی هشدارها پردازشی است برای تحلیل هشدارهای یک یا چند IDS با هدف استخراج یک دید سطح بالا از تلاش صورت‌گرفته جهت نفوذ در شبکه. سیستم‌های همبسته‌سازی هشدارها تلاش می‌کنند روابط بین هشدارها را کشف کنند تا سناریوی حمله اجراشده و هدف از آن مشخص شود. هدف اصلی این پایان‌نامه، ارائه روشی برای همبسته‌سازی بلادرنگ هشدارهای سیستم تشخیص نفوذ به منظور کشف سناریوهای حمله است.

در این تحقیق با مطالعه روش‌های موجود در همبسته‌سازی، مهم‌ترین مسائل و مشکلات مطرح در این مبحث و چالش‌های روش‌های موجود مورد بررسی قرار می‌گیرد. با توجه به نقاط قوت روش‌های سببی که در عمل کارآمدی خود را به اثبات رسانده‌اند، روش پیشنهادی این پایان‌نامه نیز بر همین اساس است. بیشتر روش‌های سببی به صورت آفلاین قابل پیاده‌سازی هستند. در کاربردهای بلادرنگ محدودیت‌های زمان و حافظه مطرح می‌شوند. در روش پیشنهادی، دانش زمینه درباره الگوی حملات در گرافی با نام گراف روابط سببی یا CRG مدل می‌شود. این گراف علاوه بر این که شامل الگوی حملات سطح پایین به صورت پیش‌نیازها و پیامدهای آنها می‌باشد، نمایشی گویا از روابط سببی بین حملات مختلف است. در روش‌های سببی با دریافت هر هشدار، جستجویی در هشدارهای قبلی و با کمک پایگاه دانش الگوی حملات با هدف یافتن هشدارهای همبسته صورت می‌گیرد. اما روش پیشنهادی ما شامل دو بخش است. قبل از ورود هرگونه هشدار، به ازای هر الگوی حمله یک جستجو برای یافتن تمام حملات همبسته با آن صورت می‌گیرد. نتیجه هر جستجو به صورت یک درخت ذخیره می‌شود. در همبسته‌سازی بلادرنگ، با دریافت هر هشدار می‌توان هشدارهای قبلی همبسته را تنها با جستجویی در درخت مربوطه پیدا نمود. بنابراین زمان پردازش هر هشدار کاهش می‌یابد. غیر از کاهش زمان پردازش، روش پیشنهادی در برابر حملات آرام نیز مقاوم است. روش پیشنهادی توسط C++ پیاده‌سازی شده و با استفاده از مجموعه داده‌های DARPA2000 تست شده است. نتایج آزمایشات انجام‌شده صحت عملکرد و کارآیی روش را از نظر زمان تأیید می‌کند.

کلمات کلیدی: ۱- حمله، ۲- نفوذ، ۳- سناریوی حمله، ۴- سیستم تشخیص نفوذ، ۵- هشدار، ۶- همبسته‌سازی هشدارها، ۷- گراف

فصل اول

مقدمه

۱ ـ مقدمه

امروزه در ماشین‌ها و شبکه‌های کامپیوتری برای مقابله با حمله‌ها از سیستم‌های امنیتی مختلفی مانند سیستم‌های تشخیص نفوذ یا IDS [1] استفاده می‌شود. در این سیستم‌ها هر گاه اتفاق مشکوکی که بیانگر یک سوء استفاده است رخ دهد، هشدارهایی [2] جهت اطلاع مدیر سیستم تولید می‌شود. مدیر سیستم برای نتیجه‌گیری از هشدارهای دریافتی و تصمیم‌گیری درباره برخورد مناسب با جریانی که شبکه را تهدید می‌کند، نیاز به تحلیل هشدارها دارد. در این راستا یکی از دغدغه‌های مدیر امنیتی شبکه کشف سناریوهای حمله [3] است، یعنی تشخیص روند پیشرفت قدم‌های یک حمله‌کننده که برای نفوذ در یک شبکه به صورت غیر مجاز طی می‌شود.

هدف ما در این پایان‌نامه بررسی نقاط ضعف و قوت روش‌های متفاوت ارائه‌شده پیرامون مبحث تحلیل هشدارهای سیستم‌های امنیتی و در نهایت ارائه روشی بلادرنگ برای کشف سناریوهای حمله از طریق همبسته‌سازی هشدارهای IDS [4] است. این فصل شامل آشنایی با مبحث تحلیل و همبسته‌سازی هشدارها و همچنین روند ارائه مطالب پایان‌نامه است.

---

[1] Intrusion Detection System
[2] Alert
[3] Attack Scenario
[4] IDS Alert Correlation

۱ ۲ امنیت شبکه‌های کامپیوتری

شبکه‌های کامپیوتری جزء اساسی جوامع امروزی محسوب می‌شوند. این شبکه‌ها معمولا به شبکه سراسری اینترنت متصل هستند و با توجه به این‌که امنیت از اهداف اولیه طراحی اینترنت نبوده است، در دهه‌های اخیر امن‌سازی این شبکه‌ها در برابر حملات از اهمیت بسیاری برخوردار شده است.

امنیت سیستم‌های کامپیوتری شامل محرمانگی[1]، صحت اطلاعات[2] و قابلیت دسترسی[3] است. تلاش برای نفوذ در یک شبکه کامپیوتری حداقل یکی از پارامترهای امنیت را به خطر می‌اندازد. این تلاش می‌تواند با هدف دسترسی غیر مجاز به اطلاعات، تغییر اطلاعات با دسترسی غیر مجاز و یا از کار انداختن سیستم (تبدیل سیستم به یک سیستم غیر قابل اعتماد یا غیر قابل استفاده) صورت گیرد [۱] عموما این تلاش‌ها به دلیل وجود آسیب‌پذیری‌هایی در سیستم شانس موفقیت دارند.

یک آسیب‌پذیری ویژگیی در طراحی نرم‌افزار یا سخت‌افزار و یا عملکرد سیستم است که سیستم را در مقابل تلاش‌های نفوذ، ناامن می‌کند. اشتباهات و یا ضعف‌هایی در پروتکل‌ها و پیاده‌سازی، نصب و یا تنظیمات سرویس‌ها و ابزارهای مختلف شبکه منجر به این آسیب‌پذیری‌ها می‌شود. مدیر امنیتی باید تاحد امکان سیستم آسیب‌پذیر را در برابر نفوذ مقاوم کند. یک حمله اجرای یک برنامه‌ی طرح‌ریزی‌شده با هدف نفوذ در شبکه است. این حمله ممکن است موفقیت‌آمیز باشد و یا با شکست مواجه شود.

با گسترش شبکه‌های کامپیوتری تعداد حملات گزارش‌شده از سال ۲۰۰۰ با سرعت زیادی رو به افزایش بوده است. بنابراین روز به روز اهمیت امنیت در شبکه‌ها بیشتر شده است. امروزه جهت تأمین امنیت در شبکه، از سیستم‌ها و ابزارهای امنیتی متفاوتی از جمله سیستم‌های تشخیص نفوذ استفاده می‌گردد.

۱ ۳ تشخیص نفوذ

با تعاریفی که در بخش ۱-۲ ارائه شد، مفهوم تشخیص نفوذ به سادگی به دست می‌آید. تشخیص نفوذ عبارت است از شناخت و کشف رفتارها و فعالیت‌هایی که منجر به خطر افتادن سه پارامتر اصلی امنیت یعنی محرمانگی، صحت اطلاعات و قابلیت دسترسی می‌شود. سیستم تشخیص نفوذ یک سیستم نرم‌افزاری و یا سخت‌افزاری و یا ترکیبی از این دو است که مسئولیت تشخیص نفوذ را به عهده دارد.

سه دهه از پیدایش سیستم‌های تشخیص نفوذ می‌گذرد. در سال ۱۹۸۰، James Anderson سندی تحت عنوان "دیده‌بانی و نظارت بر تهدیدهای امنیتی کامپیوتر"[۱] منتشر کرد که می‌توان آن را آغاز بحث تشخیص نفوذ دانست.

---

[1] Confidentiality
[2] Integrity
[3] Availability

در این سند بعد از شرح مفاهیمی مانند تهدید[۱]، خطر[۲]، آسیب‌پذیری، حمله و نفوذ به نحوه‌ی استفاده از ابزارهایی جهت دیده‌بانی و نظارت بر استفاده‌هایی که از سیستم می‌شود، اشاره شده است. پس از آن Dorothy Denning در سال ۱۹۸۷ مقاله‌ای با عنوان "مدلی برای تشخیص نفوذ"[۲] ارائه کرد، این مقاله چارچوبی برای یک سیستم تشخیص نفوذ پیشنهاد کرد که الهام‌بخش کارهای بعدی در زمینه تشخیص نفوذ شد. بعد از آن با توجه به روند روبه‌رشد گزارش رویدادها به مراکز CERT[۳] تحقیقات روی آسیب‌پذیری‌ها و روش‌های تشخیص نفوذ به طور جدی‌تر و گسترده‌ای ادامه پیدا کرد.

هنگامی که یک سیستم یا شبکه کامپیوتری تحت محافظت، مورد حمله قرار می‌گیرد، سیستم تشخیص نفوذ هشدارهایی تولید می‌کند که وقوع آن حمله را گزارش می‌دهند. حتی اگر سیستم نسبت به حمله‌ی گزارش‌شده آسیب‌پذیر نباشد، هشدار مربوطه تولید می‌شود. مدیر سیستم باید با توجه به این هشدارها تنظیمات نصب سرویس‌های موجود در شبکه را به‌گونه‌ای تغییر دهد که مقاومت کل شبکه نسبت به آن حمله افزایش یابد [۳]. بنابراین هدف از تشخیص نفوذ کشف استفاده‌های غیرمجاز، سوء استفاده و آسیب رساندن به سیستم‌ها و شبکه‌های کامپیوتری توسط هر دو دسته کاربران داخلی و مهاجمان خارجی است. در یک سیستم کامل امنیتی در کنار استفاده از دیواره‌های آتش[۴]، روش‌های رمزنگاری[۵] و تصدیق هویت[۶] که سعی می‌کنند از حمله جلوگیری کنند، از تشخیص نفوذ به عنوان دیده‌بانی برای نظارت بر نحوه استفاده از سیستم استفاده می‌شود. سیستم تشخیص نفوذ از سنسورهای نظارت کننده بر ترافیک ورودی و خروجی به سیستم یا شبکه و یا بخش های مورد نظر شبکه برای این منظور استفاده می کند. به هر نمونه IDS که در محل مناسب در شبکه یا روی یک ماشین نصب شده است یک سنسور تشخیص نفوذ گویند.

IDSها عملاً سه وظیفه‌ی کلی را برعهده دارند: شنود، تشخیص و واکنش[۷]. واکنش در مورد IDSها عموماً به ایجاد هشدار در قالب‌های مختلف محدود می‌گردد، اما دسته‌ای مشابه از ابزارهای امنیتی به نام سیستم جلوگیری از نفوذ یا IPS[۸] وجود دارند که پس از شنود و تشخیص، بسته‌های حمله‌های احتمالی را حذف می‌کنند و یا سیاست‌های سیاست‌های دیگری را در مورد حمله‌کننده به کار می‌برند. IDSها را می‌توان بر دو اساس دسته‌بندی کرد: منبع اطلاعات تشخیص و یا نوع تشخیص.

از نظر منبع اطلاعات، سیستم‌های تشخیص نفوذ در سه دسته مبتنی بر میزبان یا HIDS[۹] ، مبتنی بر شبکه یا NIDS[۱۰] و مبتنی بر منابع ناهمگون یا DIDS[۱۱] قرار می‌گیرند. در نوع مبتنی بر میزبان، برای تحلیل، از داده‌های

---

[1] Threat
[2] Risk
[3] Computer Emergency Response Team
[4] Firewall
[5] Cryptography
[6] Authentication
[7] Sniff, detection and reaction
[8] Intrusion Prevention System
[9] Host based IDS
[10] Network based IDS
[11] Distributed IDS

جمع‌آوری شده در سطح سیستم‌عامل مانند فایل‌های ثبت استفاده می‌شود. این نوع IDS وظیفه تشخیص نفوذ و حملات به یک ماشین خاص را دارد. نوع مبتنی بر شبکه شامل سیستم‌هایی است که ترافیک شبکه را به عنوان منبع اطلاعاتی مورد استفاده قرار می‌دهند، این IDSها با بررسی بسته‌ها و پروتکل‌های ارتباطات فعال، به جستجوی تلاش‌هایی که برای حمله صورت می‌پذیرد می‌پردازند. از آنجایی‌که NIDSها تشخیص را به یک سیستم منفرد محدود نمی‌کنند، عملاً گستردگی بیشتری داشته و فرایند تشخیص را به صورت توزیع‌شده انجام می‌دهند. ناکافی بودن یک نوع منبع اطلاعاتی برای تشخیص نفوذ، سیستم‌های تشخیص نفوذ را به سمت استفاده از منابع اطلاعاتی ناهمگون سوق داد. این سیستم‌ها اطلاعات را هم از میزبان و هم از شبکه جمع آوری می‌کنند. دسته ای از سیستم‌های جدید به سمت معماری توزیع شده پیش رفته‌اند (هم از نظر جمع آوری داده ها و هم از نظر تحلیل آنها). این سیستم‌ها را مبتنی بر عامل[1] گویند.

IDSها از نظر نوع تشخیص به دو دسته تقسیم می‌شوند:

۱ - مبتنی بر الگو[2]: این IDSها بر اساس الگوهای حمله‌های شناخته‌شده کار می‌کنند. سیستم‌های مبتنی بر حملات شناخته‌شده از یک پایگاه قوانین استفاده می‌کنند. این قوانین مشخص می‌کند که چه نوع استفاده‌هایی مجاز نیست. در این سیستم‌ها قوانین با توجه به استفاده صحیح از پروتکل‌ها و سرویس‌ها تعریف می‌شوند. الگوی هرگونه استفاده ناصحیح به صورت یک قانون نوشته می‌شود. عدم انطباق با همه قوانین نشان‌دهنده مجاز بودن آن دسترسی و یا استفاده است.

۲ - مبتنی بر ناهنجاری[3]: این IDSها بر اساس تشخیص رفتارهای غیرمعمول کار می‌کنند. سیستم‌های مبتنی بر بدرفتاری، مدلی از ترافیک و یا استفاده مجاز و طبیعی بدست می‌آورند. هر آن‌چه از آن مدل طبیعی فاصله بگیرد حمله شناخته می‌شود.

سیستم‌های مبتنی بر ناهنجاری قادر به تشخیص حمله‌های جدید هم خواهند بود، در صورتی که سیستم‌های مبتنی بر الگو، تنها حمله‌هایی را تشخیص می‌دهند که از نوع حملات شناخته‌شده‌ای باشند که قانون مربوط به آن‌ها در پایگاه قوانین وجود داشته باشد. اما از طرف دیگر در عمل خطای سیستم‌های مبتنی بر ناهنجاری خیلی بیشتر از خطای سیستم‌های مبتنی بر الگو است و نوع حمله یا تلاش انجام‌شده هم مشخص نیست. اکثر سیستم‌های تشخیص نفوذ کاربردی، بر اساس الگو کار می‌کنند.

---

[1] Agent Based
[2] Signature or Misused Detection Based
[3] Anomaly Detection Based

۱ ٤ چالش‌های سیستم‌های تشخیص نفوذ

در عمل هنگام استفاده از سیستم‌های تشخیص نفوذ با مشکلاتی مواجه می‌شویم. در سال ۲۰۰۱، Debar مشکلاتی را در ارتباط با سیستم‌های تشخیص نفوذ بیان نمود [۴] و سپس روش‌هایی برای حل آن مشکلات پیشنهاد کرد. با توجه به دسته‌بندی Debar و نیز با بررسی‌های بعدی در زمینه IDS این مشکلات عبارتند از:

۱ - جریان سیل‌آسای هشدارها[1]: IDS تعداد بسیار زیادی هشدار مستقل از هم تولید می‌کند. برای مدیر سیستم، کنترل و تحلیل این تعداد زیاد هشدار کار دشوار وگاه بدون ابزار دیگری غیر ممکن است. در بعضی از شبکه‌ها چندین سنسور در نقاط مختلف شبکه قرار می‌گیرد. گاهی حتی در این سنسورها IDSهای متفاوت با قوانین و مکانیزم‌های مختلف تشخیص، نصب می‌شود. بنابراین روزانه تعداد صدها یا هزاران هشدار تولید می‌شود. این تعداد بسیار زیاد نشانه تعداد زیاد حمله نیست، بلکه به دلیل وجود هشدارهای غلط و یا تکراری می‌باشد. با توجه به وجود حمله‌هایی که با هدف گمراهی IDS سعی در تولید تعداد زیاد هشدارهای بیهوده و نامربوط می‌کنند، این مشکل IDS جدی‌تر می‌شود.

۲ - هشدارهای غلط تولیدشده[2]: از آن‌جایی که گاهی قوانین IDS به اندازه کافی دقیق نیستند و مرز دقیقی بین رفتارها و ترافیک عادی و غیر عادی وجود ندارد، امکان تولید هشدارهای غلط زیاد است. برای مثال در NIDSها ممکن است قوانینی داشته باشیم که با دیدن بسته‌های مشکوک هشدار دهند، اما لزوما وجود الگوی هر رفتار مشکوکی تأییدکننده رخداد آن حمله نیست. همچنین به دلیل وجود هر مشکل دیگری در پیاده‌سازی یک IDS، ممکن است هشدارهای اشتباهی تولید شود. این هشدارهای اشتباه همان تشخیص‌های مثبت غلط[3] سیستم هستند. هشدارهای صحیح مربوط به حمله‌های واقعی اتفاق‌افتاده هم در بین صدها هشدار اشتباه قرار می‌گیرند. بنابراین مدیر سیستم به سختی می‌تواند جریان‌های واقعی حمله را تشخیص دهد.

۳ - هشدارهای مفقودشده[4]: IDS به دلایل مختلف ممکن است متوجه رخداد حمله‌ای نشود و به همین دلیل هشدار مربوطه را تولید نکند. برای مثال گاهی حمله‌کننده روش‌هایی را برای پنهان‌کردن حمله خود به کار می‌برد. تعریف نادقیق قوانین هم می‌تواند منجر به از دست‌رفتن هشدار شود. این هشدارهای مفقودشده همان تشخیص‌های منفی غلط[5] سیستم هستند.

۴ - هشدارهای مربوط به حملات ناموفق: گاهی حمله‌کننده، حمله‌ای را روی یک شبکه اعمال می‌کند، ولی آسیب‌پذیری مربوطه و یا شرایط لازم روی ماشین هدف وجود ندارد، بنابراین حمله ناکام می‌ماند. اما به دلیل

---

[1] Alerts Flooding
[2] False Alerts
[3] False Positive
[4] Missed Alerts
[5] False Negative

وجود الگوی حمله مفروض، IDS هشدار مربوطه را تولید می‌کند. برای مثال اگر حمله‌کننده‌ای در حال تلاش برای بهره‌برداری از یک آسیب‌پذیری مربوط به سرور وب IIS باشد، IDSای که اطلاعاتی راجع به شبکه ندارد هشدارهای مربوطه را که اتفاقا اولویت بالایی از لحاظ میزان خطر دارند، تولید می‌کند. اما اگر سیستم تحت حمله دارای سرور وب آپاچی[1] باشد، هشدارهای تولیدشده اهمیت خاصی ندارند. به اصطلاح گفته می‌شود که هشدارها بعد از تولید نیاز به تأیید دارند.

۵ - عدم تشخیص همبستگی بین هشدارها: IDS هشدارهایی را مستقل از یکدیگر و بدون در نظر گرفتن امکان وجود رابطه منطقی بین هشدارها تولید می‌کند. در واقع هر یک از هشدارها فقط می‌توانند وقوع یک حمله سطح پایین را به ما اطلاع دهند. بیشتر حمله‌های ماهرانه در چندین مرحله و طی یک سناریوی برنامه‌ریزی شده صورت می‌گیرند. مدیر سیستم بدون تحلیل و به کاربردن ابزار مناسب قادر به تشخیص همبستگی بین هشدارها نیست.

۶ - آگاهی بعد از وقوع حادثه: یک IDS به خودی خود تنها قادر به تشخیص وقوع حمله است، یعنی پس از آن که یک حمله یا تهدید اعمال شد هشداری مبنی بر وقوع آن داده می‌شود. در چنین IDSای امکان پیش‌بینی وقوع یک حمله وجود ندارد.

با توجه به مشکلاتی که ذکر شد، در صورتی که بخواهیم از هشدارهای IDS جهت تصمیم‌گیری در IPS استفاده کنیم، نمی‌توانیم تنها به هشدارهای IDS اطمینان و اکتفا کنیم. در شبکه‌های بزرگ برای زیر نظرداشتن تمام ترافیک شبکه سنسورهای مختلفی از IDSها (شامل NIDS و HIDS) در مکان‌های مختلف شبکه قرار می‌گیرد. هشدارهایی که در تمام این سنسورها تولید می‌شوند، باید در یک مرکز جمع‌آوری شود و تحلیل‌های بعدی صورت گیرد. بدون سازماندهی و تحلیل تعداد بسیار زیاد هشدارهای جمع‌آوری‌شده از سنسورهای مختلف که حاوی هشدارهای غلط نیز هستند، نمی‌توان تصمیم قطعی در رابطه با نحوه برخورد با حمله گرفت. از طرفی بر اساس اصل "پیشگیری بهتر از درمان" بهتر است سعی کنیم قبل از وقوع آخرین مرحله یک سناریوی حمله که هدف نهایی یک حمله‌کننده است، وقوع آن را پیش‌بینی کنیم.

۱ ۵ سیستم همبسته‌سازی[2] هشدارهای IDS

سیستم همبسته‌سازی هشدار برای حل مشکلات IDS پیشنهاد شده است. سیستم‌های همبسته‌ساز، هشدارها را از سنسورهای مختلف دریافت می‌کنند و با تحلیل و بررسی آنها یک دید سطح بالا از وضعیت امنیتی شبکه ارائه

---

[1] Apache
[2] Alert Correlation System (ACS)

می‌دهند. این مجموعه تحلیل‌ها شامل روش‌هایی برای انبوهش هشدارها[۱]، هم‌جوشی هشدارها[۲]، کاهش افزونگی هشدارها[۳]، حذف هشدارهای غلط، کشف هشدارهای مفقودشده[۴] و در نهایت بدست آوردن همبستگی‌های موجود بین هشدارها جهت تشخیص سناریوی حمله و پیش‌بینی رخداد حمله می‌باشند.

همان‌طور که گفته شد بیشتر حمله‌های ماهرانه در چندین مرحله و طی یک سناریوی برنامه‌ریزی شده صورت می‌گیرند. عموما هدف یک حمله‌کننده از نفوذ در یک شبکه به دست‌آوردن یک دسترسی غیرمجاز به شبکه و یا ایجاد اختلال در شبکه است. حمله‌کننده برای رسیدن به هدف نهایی باید ابتدا مراحل ابتدایی را بگذراند. او در هر یک از مراحل ابتدایی اطلاعاتی درباره شبکه و یا ماشین موردنظرش پیدا می‌کند. اجرای هر مرحله مستلزم اجرای مرحله قبل است. بدین‌ترتیب حمله‌کننده قدم به قدم به هدف نهایی خود نزدیک می‌شود.

برای روشن‌شدن مطلب به مثالی ساده از [۵] اشاره می‌شود. حمله‌کننده ابتدا شبکه‌ای را برای جستجوی ماشین‌های با آسیب‌پذیری مورد نظرش پویش[۵] می‌کند. معمولا پویش، اولین مرحله یک سناریوی حمله است. حمله‌کننده بعد از پیداکردن ماشین‌های آسیب‌پذیر حمله‌ای را روی سرور ftp اعمال می‌کند، اما این حمله ناموفق می‌شود. بنابراین بار دوم همان تلاش را با به‌کار بردن پارامترهای دیگر تکرار می‌کند و این بار موفق می‌شود. بعد از شکست ورودی[۶]، ابزارهای حمله موردنظر را روی سرور نصب و شروع به پویش شبکه داخلی می‌کند. در مراحل بعدی، حمله‌کننده می‌تواند به دسترسی‌های دیگر مورد نیازش برسد و فایل‌های موردنظرش را بدون داشتن دسترسی مجاز روی ماشین‌ها اجرا کند.

سنسورهای IDS که در نقاط مختلف شبکه نصب شده‌اند متوجه بعضی و یا همه مراحل حمله به طور جداگانه می‌شوند و هشدارهای مربوطه را تولید می‌کنند. بعضی از سنسورها ممکن است با هر تلاش برای پویش، تعداد زیادی هشدار تولید کنند. اما مدیر سیستم باید تنها یک هشدار برای تمام این مرحله دریافت کند. یعنی پویش‌های متفاوت باید در یک گروه جمع‌بندی شوند و یک هشدار سطح بالا برای اعلان کل مرحله پویش به مدیر سیستم داده شود. هشدارهای مربوط به مرحله‌ای که ناموفق شد باید حذف شوند و در نهایت تمام هشدارهای مربوط به این سناریو به صورت دنباله منظمی از هشدارهای سطح بالا با هم همبسته‌سازی شوند. اگر سناریو را تا مرحله پویش شبکه داخلی در نظر بگیریم هشدارها باید در سه مرحله پویش، شکست ورودی و نصب ابزار و پویش داخلی دسته‌بندی و همبسته‌سازی شوند.

---

[1] Alert Aggregation
[2] Alert Fusion
[3] Alert Reduction
[4] Missed Alerts discovery
[5] Scan
[6] Break in

همان‌طور که از مثال گذشته مشخص است عملیات متفاوتی روی هشدارها باید صورت گیرد تا گزارش مطلوب نهایی به مدیر سیستم برسد. مقاله [۶] طرح یک سیستم جامع همبسته‌ساز هشدارها را ارائه می‌دهد. این سیستم شامل تمام قسمت‌هایی است که برای یک سیستم جامع تحلیل هشدارها لازم می‌باشد. مطالعه این مقاله برای درک کلی از مراحل مختلف مورد نیاز برای تحلیل هشدارها مفید است (که در فصل دوم بدان پرداخته خواهد شد). البته در روش‌هایی که ارائه می‌شوند، معمولا هر چند مرحله مفروض در [۵] در یک مرحله انجام می‌شود.

۱ ۵ ۱ روش‌های همبسته‌سازی هشدارها

تاکنون روش‌های مختلفی برای همبسته‌سازی هشدارها ارائه شده است. هر یک از این روش‌ها معمولا یک یا چند هدف از اهداف همبسته‌سازی هشدارها را در نظر دارد. به طور کلی روش‌های ارائه‌شده در زمینه تحلیل هشدارها را می‌توان در چند گروه دسته‌بندی کرد:

۱ - روش‌هایی مبتنی بر تشابه ویژگی‌های هشدارها: در این روش‌ها هشدارها را بر اساس بعضی پارامترهایشان در گروه هایی دسته بندی می‌کنند. برای مثال بر اساس میزان تشابه آدرس IP مقصد یا منبع و یا شماره پورت، هشدارها در دسته‌های مختلف قرار می‌گیرند. روش‌های مختلف آماری،احتمالی و بیشتر روش‌های شبکه عصبی و داده‌کاوی از این دسته‌اند. اما این روش فقط به عنوان یک پیش‌پردازش برای به دست‌آوردن همبستگی هشدارها مناسب است. روش‌هایی که در [۱۰,۹,۸,۷] ارائه شده‌اند در این دسته قرار می‌گیرند.

۲ - روش‌های مبتنی بر الگوهای موجود سناریوهای حمله: این روش‌ها از دانش زمینه ما درباره استراتژی‌ها و سناریوهای حمله شناخته‌شده استفاده می‌کنند. این سناریوها به طور دستی یا از طریق روش‌های یادگیری طی آموزش یک سیستم برای شبکه مفروض بدست می‌آیند. مبنای این روش‌ها مانند مبنای IDSهای مبتنی بر الگو است. روشن است که این روش‌ها محدود به یک سری سناریوهای شناخته شده می‌شوند. روش‌هایی که از تعریف یک زبان برای مدل‌کردن پایگاه داده الگوها استفاده می کنند، در این دسته قرار می‌گیرند، از جمله LAMDBA [۱۱] و STATL [۱۲]. گاهی روش‌های یادگیری ماشین و داده‌کاوی برای همبسته‌سازی هشدارها بر اساس دانشی که از دنبال‌کردن مجموعه داده‌های حاوی سناریوهای حمله به‌دست می‌آید، به کار می‌رود [۱۳].

۳ - روش های سببی[1]: با توجه به محدودیت‌ها و مشکلات روش دوم، روش‌های دیگری مطرح شدندکه در آن‌ها سناریوها را به صورت یک چندتایی از انواع هشدار تعریف می‌کنند. این روش بر این اساس است که هشدارها مستقل از هم نیستند، بلکه هشدارها مربوط به مراحل مختلف یک حمله هستند. در این روش‌ها از

[1] Causal Approach

پیش‌نیازها[1] و پیامدهای[2] حمله‌ها برای همبسته‌سازی استفاده می‌شود. بدین صورت که ابتدا پایگاه داده ای از حمله‌ها و پیش‌نیازها (شرایط لازم برای امکان اجرای حمله) و پیامدهای (شرایط بدست‌آمده از اجرای حمله) آنها ساخته می‌شود و سپس هشدارهای ورودی در صورتی همبسته می‌شوند که پیش‌نیاز بعضی هشدارهای بعدی از پیامد هشدارهای قبلی بدست آید. هر چند این روش‌ها محدودیت کمتری نسبت به دو روش قبل در کشف سناریوهای حمله دارند، اما برای تعریف پایگاه داده موردنظر به دانش کافی درباره حمله‌ها و هشدارهای مربوطه نیاز است. مبنای روش‌های ارائه‌شده در این دسته مدل requires/provides است که توسط Templeton ارائه شده است[۱۴]. از جمله روش‌هایی که در این دسته قرار می‌گیرند، روش‌های ارائه‌شده توسط Ning [۱۶,۱۵] و Cuppens [۱۷] هستند.

۴ - روش‌های هیبرید: در این روش‌ها ترکیبی از روش‌های ذکرشده مبتنی بر الگو و سببی و نیز روش‌های آماری به کار خواهد رفت. گاه هشدارهای تشخیص داده شده و نتایج همبسته‌سازی با فایل‌های ثبت سیستم تطبیق داده می‌شوند، مثلا رویدادهای سیستم عامل با توجه به نتایج دنبال و صحت آن‌ها بررسی می‌شود [۱۹,۱۸].

۵ - روش‌های مبتنی بر آسیب‌پذیری‌ها[3]: در این روش‌ها علاوه بر داشتن پایگاه داده‌ای از الگوهای حمله و به کاربردن روش‌های سببی یا روش‌های دیگر، آسیب‌پذیری‌های موجود در شبکه را نیز در نظر می‌گیرند [۲۰]. در نظر گرفتن آسیب‌پذیری‌های موجود در شبکه راهکاری برای حذف هشدارهای مربوط به حملات ناموفق و نامربوط به شرایط شبکه مفروض است.

این دسته‌بندی روش‌ها به نوعی ترتیب زمانی مطالعات و پژوهش‌ها را نیز در زمینه همبسته‌سازی هشدارها نشان می‌دهد. البته هنوز هم ممکن است از روش‌های ۱ و ۲ استفاده شود، اما روش‌های بعدی پیشرفته‌تر محسوب می‌شوند و روش‌های دسته اول هم به صورت پیش‌پردازشی برای به‌کار بردن روش‌های دیگر به کار می‌روند.

۱.۶ اهداف پایان‌نامه

در این تحقیق با مطالعه روش‌های موجود در همبسته‌سازی، مهم‌ترین مسائل و مشکلات مطرح در رابطه با همبسته‌سازی مورد بررسی قرار گرفت. یکی از مشکلات روش‌های موجود ناتوانی آنها در بررسی بلادرنگ هشدارها است. بیشتر روش‌های ارائه‌شده توانایی تشخیص همبستگی‌ها همزمان با ورود هشدارها را ندارند، یعنی به صورت آفلاین[4] کار می‌کنند. در این روش‌ها همبسته‌سازی روی مجموعه‌ای از هشدارهای موجود انجام می‌شود. اما در عمل

---

[1] Prerequisite
[2] Consequence
[3] Vulnerability-centric
[4] Offline

با جریانی از هشدارها مواجه هستیم و با ورود هر هشدار باید همبستگی آن با هشدارهای قبلی بررسی شود. در همبسته‌سازی بلادرنگ مسائل مهمی از جمله کارآمدی از نظر زمان و حافظه مطرح می‌شود. همچنین در همبسته‌سازی هشدارها به صورت آفلاین پیش‌بینی رخداد حمله مفهومی ندارد، در صورتی که یکی از اهداف مهم در تحلیل هشدارها پیش‌بینی مرحله‌ای از حمله است که احتمال وقوع آن در آینده نزدیک زیاد است.

از طرفی بیشتر روش‌ها تنها به بعضی از تحلیل‌های لازم برای همبسته‌سازی هشدارها که در بخش ۱- ۵ به آنها اشاره شد، می‌پردازند. مدل‌های کاملی هم که تاکنون ارائه شده‌اند، تحلیل‌های لازم را در چندین مرحله انجام می‌دهند. برای مثال ابتدا عمل دسته‌بندی و فشرده‌سازی را انجام می‌دهند، سپس سعی می‌کنند هشدارهای غلط را حذف کنند و در نهایت سناریوی حمله را استخراج می‌کنند. در یک سیستم بلادرنگ انتظار داریم همه این مراحل به صورت همزمان انجام شوند.

در این پایان‌نامه پس از بررسی نقاط ضعف و قوت روش‌های متفاوت ارائه‌شده، یک سیستم همبسته‌سازی هشدار را ارائه و پیاده‌سازی خواهیم کرد که اهداف زیر را برآورده کند:

۱ - بلادرنگ باشد.

۲ - هزینه‌ی زمان و حافظه در آن برای یک سیستم بلادرنگ قابل قبول باشد.

۳ - در برابر تعداد زیاد هشدارها، هشدارهای غلط، حمله‌های گمراه‌کننده و حمله‌های آرام مقاوم باشد.

از طرفی سعی بر آن است که مدل ارائه‌شده برای سیستم پیشنهادی قابلیت کشف هشدارهای مفقودشده و پیش‌بینی رخداد حملات را نیز داشته باشد.

۱ ۴ روند ارائه مطالب

مطالب این پایان‌نامه به صورت زیر ارائه شده‌اند: ابتدا در فصل دوم مرور کوتاهی بر مقدمات لازم برای مطالعه بحث تحلیل هشدارهای امنیتی خواهیم داشت. فصل سوم شامل مطالعه و تحلیل جامعی از روش‌های موجود ارائه‌شده در زمینه‌ی همبسته‌سازی هشدارها می‌باشد. در فصل چهارم سیستم پیشنهادی شرح داده می‌شود و مورد بررسی قرار می‌گیرد. در بخش آخر فصل چهارم نتایج عملی روش پیشنهادی ارائه می‌شود. در نهایت، در فصل پنجم به نتیجه‌گیری و کارهای آتی می‌پردازیم.

فصل دوم
پیش‌زمینه

۲ ـ مقدمه

مطالعه و پژوهش در زمینه‌ی تحلیل هشدارهای سیستم‌های تشخیص نفوذ نیاز به دانش پیشین درباره امنیت شبکه، آسیب‌پذیری‌ها، حمله‌ها و سیستم‌های تشخیص نفوذ دارد. هر یک از این موارد، خود مبحث گسترده و پیچیده‌ای را شامل می‌شود که از بحث این پایان‌نامه خارج است. در فصل مقدمه به طور گذرا به بعضی از مفاهیم اشاره شد. در این فصل به صورت مفصل‌تر به شرح آسیب‌پذیری‌ها، حمله و نفوذ، سیستم‌های تشخیص نفوذ و تحلیل هشدارهای امنیتی در شبکه می‌پردازیم.

همچنین در بخش آخر فصل، یک مدل عمومی برای همبسته‌سازی هشدارها شرح داده می‌شود. این مدل شامل مجموعه جامعی از اجزاء لازم برای یک سیستم تحلیل هشدارها و چارچوبی بر اساس آن مدل است. مطالعه این مدل یک دید کلی نسبت به اعمال مختلفی که ممکن است جهت تحلیل هشدارها صورت گیرد، به خواننده می‌بخشد.

۲ ـ تعریف امنیت شبکه

بر اساس تعاریفی که در سند [۲۱] درباره امنیت کامپیوتر ارائه شده است، می‌توان گفت برای هر شبکه کامپیوتری تعدادی اعمال (و یا حالت‌ها) مجاز و بقیه غیر مجاز تلقی می‌شوند. یک سیاست امنیتی که مشخص می‌کند چه چیز مجاز و چه چیز غیر مجاز است، امنیت شبکه را تعریف می‌کند. اگر سیستم (شامل تمام ماشین‌های موجود در شبکه و