دانشگاه یزد

دانشکده مهندسی برق و کامپیوتر

گروه مهندسی کامپیوتر

پایان‌نامه

برای دریافت درجه کارشناسی ارشد

مهندسی فناوری اطلاعات- شبکه‌های کامپیوتری

بررسی روش‌های کاهش هشدارهای غلط در تشخیص نفوذ

استاد راهنما:

دکتر فضل‌ا... ادیب‌نیا

اساتید مشاور:

دکتر ولی درهمی

سیدهادی سجادی

پژوهش و نگارش:

سارا خانچی

مهر ۸۸

تقدیم به

مادر دلسوزم و **پدر مهربانم**

کسانی که در هر گام از زندگانیم، سایه‌بان و پشتیبانم بودند.

تقدیر و تشکر

آفرین جان آفرین پاک را
آنکه جان بخشید و ایمان خاک را

برگ دیگری از زندگی‌ام همراه با ورق خوردن صفحات این پایان‌نامه ورق خواهد خورد. در این مسیر، عزیزانی همراهیم کردند که حرمت همراهی و کسب فیض از حضورشان، آدمی را به تشکر وا می‌دارد.

در آغاز سپاس خود را از استاد گرانقدرم، جناب آقای دکتر ادیب‌نیا اعلام می‌دارم. باشد که این کلام، الطاف ایشان در مسیر تامین این پایان‌نامه را بارز کند.

از استاد مشاور محترم، جناب آقای دکتر درهمی نیز تقدیر و تشکر می‌نمایم. راهنمایی‌های قابل تقدیر ایشان، توانست هادی راهم در تالیف این پایان‌نامه باشد.

همچنین از آقای دکتر صرام و آقای دکتر المدرسی که قبول زحمت داوری این پایان‌نامه را بر دوش کشیدند، صمیمانه تشکر می‌نمایم.

در انتها، سپاسی را با تمام وجود از دو عزیزی دارم که از آغاز همراه و همیارم بودند، مادر صبورم و پدر دوست‌داشتنی‌ام؛ که گرمی نفسم از گرمای محبتشان است و بیش از لحظه لحظه زندگی‌ام مدیون همراهی و همیاریشان هستم.

و تشکر بی شائبه من از تمامی کسانی است که در مسیر زندگیم، چون استادی ناب، کلامی به من آموختند.

چکیده

در جوامع امروزی، امنیت شبکه‌های کامپیوتری و اینترنت به مقوله مهمی در بین متخصصین این امر بدل گشته است. گسترش سریع و روزافزون شبکه‌های کامپیوتری سبب شده تا حملات شبکه‌ای نیز به همان میزان از پیچیدگی قابل توجهی برخوردار گردند. با توجه به اینکه امور روزمره مردم به شدت به کامپیوترها و شبکه‌های کامپیوتری وابسته است و با گسترش جرایم الکترونیکی، نیاز به ابزارهای قدرتمندی است که بتوانند امنیت را در سطوح بالا فراهم آورند. در دو دهه اخیر سیستم‌های تشخیص نفوذ این مسئولیت را برعهده گرفته‌اند. یکی از مشکلات اساسی که امروزه سیستم‌های تشخیص نفوذ تجاری با آن روبه‌رو هستند، نرخ بالای هشدارهای تولیدی است که اکثر آن‌ها را هشدارهای نادرست تشکیل می‌دهند در این پایان‌نامه این معضل مورد بررسی قرار گرفته و راه‌کاری برای کاهش حجم وسیع هشدارهای نادرست ارائه گردیده است. روش پیشنهادی در مرحله اول، تحلیل فرکانسی، با تحلیل فرکانسی خصوصیات هشدارها، خصوصیات تکرارشونده را به عنوان خصوصیات هشدارهای نادرست در مجموعه‌ای گردآوری می‌کند. در مرحله دوم، تشخیص برخط، با استفاده از این مجموعه، هشدارهای تازه‌رسیده را امتیازبندی کرده و بر اساس آن هشدارهای نادرست را فیلتر می‌نماید. سیستم پیشنهادی توسط مجموعه داده DARPA 2000 مورد تست و ارزیابی قرار گرفت. کاهش ۸۷٪ هشدارهای نادرست و تشخیص ۱۰۰٪ هشدارهای درست، نشان‌دهنده کارآیی بالای سیستم و قابلیت کاربردی آن می‌باشد.

کلمات کلیدی: تشخیص برخط، تشخیص نفوذ، فرکانس، مجموعه داده DARPA 2000، هشدار نادرست

فهرست مندرجات

لیست اشکال

لیست جداول

فهرست اختصارات

فصل ۱

مقدمه

۱.۱ مقدمه

گسترش شبکه‌های کامپیوتری و استفاده گسترده از اینترنت توسط درصد عظیمی از اقشار مختلف اجتماع، امنیت سیستم‌ها را بیش از پیش با خطر مواجه ساخته است. در موارد بسیاری فعالیت‌های غیرقانونی از خارج شبکه و حتی توسط افراد مغرض در شبکه صورت می‌گیرد. رشد و گسترش روزافزون نفوذها و جرایم الکترونیکی و خسارات ناشی از آن بر اقتصاد، ثابت نمود که به‌کارگیری روش‌های امنیتی پیشین همچون رمزنگاری[۱]، اعتبارسنجی[۲] و دیواره آتش[۳] به تنهایی جهت جلوگیری از نفوذ کافی نمی‌باشد. بنابراین لزوم طراحی و به‌کارگیری ابزار و روش‌های نوین و قدرتمند جهت حفظ امنیت شبکه‌ها که بتوانند در کنار روش‌های کلاسیک امنیت دلخواه را تامین نمایند، ضروری به‌نظر می‌رسید. سیستم‌های تشخیص نفوذ[۴] این مسئولیت را در شبکه‌های کامپیوتری بر عهده گرفتند.

سیستم‌های تشخیص نفوذ، ابزارهای امنیتی مهم در دوره اخیر می‌باشند که امنیت را در سطوح بالا برای ما فراهم می‌آورند. بر اساس نتایج بررسی‌های جرم‌های FBI/CSI و امنیت کامپیوتر در سال ۲۰۰۶، سیستم‌های تشخیص نفوذ در میان پراستفاده‌ترین فناوری‌های امنیتی، رتبه پنجم را در میان پاسخگویان کسب کرده‌اند(۹۶٪ سازمان‌های مورد بررسی

[۱] Cryptography

[۲] Authentication

[۳] Firewall

[۴] Intrusion Detection Systems(IDSs)

از سیستم‌های تشخیص نفوذ به عنوان راه‌حل امنیتی استفاده می‌کنند). نفوذ، به هرگونه تلاش جهت اختلال در هر یک از رکن‌های اساسی امنیت یعنی صحت، قابلیت اطمینان و دسترسی‌پذیری به یک منبع کامپیوتری، گفته می‌شود[۱]. هدف سیستم‌های تشخیص نفوذ کشف این‌گونه تلاش‌ها و معرفی آن به تحلیل‌گران از طریق هشدار می‌باشد تا اقدامات لازم جهت جلوگیری از آن به عمل آید و در بعضی موارد خود اقدامات اولیه از قبیل قطع اتصال را انجام می‌دهد.

از زمان ارائه سیستم‌های تشخیص نفوذ تا به امروز، این سیستم‌ها با مشکلات چندانی روبه‌رو بوده‌اند که با تحقیقات انجام شده و بهبودهای صورت گرفته در جهت رفع مشکلات آن‌ها، روز به روز به سمت تکامل خود پیش می‌روند. یکی از مشکلات اساسی که امروزه با وجود به‌کارگیری گسترده، سیستم‌های تشخیص نفوذ تجاری با آن مواجه هستند، تعداد زیاد هشدارها و بالابودن نرخ تشخیص نادرست در بین هشدارها می‌باشد[۲، ۳]. طبق ادعای Julisch[۴]، بیش از ۹۰٪ این هشدارها نادرست می‌باشند که به پیامدهای امنیتی مربوط نمی‌باشند.

۲.۱ هشدارهای نادرست در سیستم‌های تشخیص نفوذ

هشدار نادرست به هشدار حمله‌ای گفته می‌شود که اشتباه اعلام گردیده و نیاز به توجه تحلیل‌گر تشخیص نفوذ دارد. تحلیل‌گر تشخیص نفوذ شخصی است که وظیفه‌ی او بررسی هشدارهای سیستم تشخیص نفوذ و جلوگیری از وقوع یا گسترش نفوذ در شبکه‌های کامپیوتری می‌باشد.

همانطور که گفته شد سیستم‌های تشخیص نفوذ تجاری که امروزه از آن‌ها استفاده می‌شود، هشدارهای زیادی ایجاد می‌کنند. حجم وسیع هشدارها مشکلات زیادی را برای تحلیل‌گران هشدار به‌وجود آورده است. در اکثر مواقع تحلیل‌گران به علت هجوم سیل عظیمی از هشدارها نمی‌توانند آن‌ها را به دقت و به صورت بلادرنگ پردازش نموده و تحلیل نمایند. این امر سبب می‌گردد تا در بعضی مواقع حملات اصلی در زیر کوهی از هشدارهای مربوط به وقایع بی‌خطر، دفن گردند و یا زمانی به وجود آن‌ها پی برده شود که فرصتی جهت مقابله با

اثرات آن‌ها نباشد. به عبارت دیگر، حجم هشدارهای نادرست اعلام شده توسط این سیستم‌ها نسبت به هشدارهای درست بسیار بیشتر می‌باشد و عملا هشدارهای درست در مقابل آن‌ها ناچیز شمرده می‌شوند. سیستم‌های تشخیص نفوذ زمانی کارآیی خود را حفظ می‌کنند که بتوانند علاوه بر تشخیص نفوذها، حجم این هشدارهای نادرست را در سطح قابل قبولی نگه دارند. ساخت سیستم‌های تشخیص نفوذی که بتوانند هشدارهای نادرست کمی ایجاد کنند، دشوار می‌باشد. علت‌های این امر در زیر بیان گردیده است[۵]:

محدودیت‌های زمان اجرا: در موارد زیادی، نفوذ تنها به مقدار کمی از فعالیت‌های عادی[۱] متفاوت است. در بعضی مواقع نفوذ بودن یک فعالیت تنها توسط شرایطی که در آن رخ می‌دهد، تعیین می‌گردد. از آن‌جایی که سیستم‌های تشخیص نفوذ باید بلادرنگ باشند، قادر نیستند متن همه‌ی فعالیت‌ها را با دقت بالا مورد تجزیه و تحلیل قرار دهند.

اختصاصی بودن امضاهای تشخیص: نوشتن امضا برای سیستم‌های تشخیص نفوذ کار دشواری است. در صورتی که امضا خیلی خاص طراحی شود نمی‌تواند همه‌ی حملات یا انواع آن را ضبط کند و یک امضای بسیار کلی تنها اقدامات مجاز را از نفوذها تشخیص می‌دهد.

اگر امضا خیلی خاص طراحی شود امکان عدم تشخیص حملات، بالا می‌رود. در سیستم‌های تشخیص نفوذ عدم تشخیص حمله از تشخیص اشتباه اتصال عادی به عنوان حمله، خطرناک‌تر می‌باشد. در صورت کلی بودن امضا نیز حس‌گرهای تشخیص به ازای همه‌ی بسته‌هایی که با امضا تطبیق یابند، هشدار حمله مربوطه را ایجاد و اعلام می‌کنند. در این حالت هر حس‌گر هزاران هشدار بی‌خطر تولید می‌کند . اگر مهاجم از این موضوع اطلاع یابد سعی می‌کند با ارسال بسته‌هایی که این خاصیت را ایجاد می‌نماید، موجب ایجاد سیل عظیمی از هشدارهای نادرست گردد. در بعضی موارد، برقراری تعادل بین این دو مورد مشکل است.

وابستگی به محیط: عملیاتی که در محیط‌های مشخصی عادی می‌باشد، ممکن است در

[۱] Normal

محیط‌های دیگر بدخواه باشد. به عنوان مثال پویش[۱] شبکه یکی از مراحل اولیه اجرای حملات شبکه‌ای است، تنها در صورتی این عمل بدخواه نیست که کامپیوتر مورد نظر مجاز به انجام چنین عملی باشد.

مبنای هشدارهای نادرست[۲]: از دیدگاه آماری و مثال زیر، می‌توانیم احتمال نادرست بودن هشدار را با استفاده از تئوری بیز [۳] محاسبه کنیم. فرض کنید که ما در روز ۱,۰۰۰,۰۰۰ بسته را تحلیل می‌کنیم که تنها ۲۰ بسته‌ی آن نفوذ می‌باشند که احتمال نفوذ $P(I) = ۲ \times ۱۰^{-۵}$ می‌گردد. با داشتن نرخ تشخیص حس‌گر $(P(A|\neg I))$ و نرخ تشخیص نادرست آن $(P(A|I))$، می‌توانیم از تئوری بیز برای محاسبه نرخ تشخیص بیزی $(P(A|\neg I))$ استفاده کنیم. به بیان دیگر احتمال اینکه یک هشدار واقعا نشان‌دهنده نفوذ باشد:

$$P(I|A) = \frac{P(I).P(A|I)}{P(I).P(A|I) + P(\neg I).(P(A|\neg I)} \qquad (۱.۱)$$

با استفاده از احتمال نفوذ بیان شده $P(I) = ۲ \times ۱۰^{-۵}$ و با فرض نرخ تشخیص غیرواقعی $P(A|I) = ۰/۱$ و تشخیص اشتباه بسیار کم از مرتبه $P(A|\neg I) = ۱۰^{-۵}$ خواهیم داشت $P(A|\neg I) = ۰/۶۶$، یعنی یک سوم کل هشدارها مربوط به فعالیت‌های نفوذ نمی‌باشند. با نرخ تشخیص اشتباه یکسان و نرخ تشخیص واقعی‌تر ۰/۷، ۲۴٪ هشدارها نادرست خواهند بود.

۳.۱ شیوه‌های کاهش میزان هشدار نادرست

در این بخش به صورت کلی انواع راه‌حل‌هایی بیان می‌گردند که جهت کاهش هشدارهای نادرست در سیستم‌های تشخیص نفوذ می‌توانند مورد استفاده قرار بگیرند. این راه‌کارها از

[۱] Scan

[۲] Base Rate Fallacy

[۳] Bayes

جنبه‌های مختلف امکان کاهش هشدارها را مورد بررسی قرار می‌دهد.

الف. بهبود سیستم‌های تشخیص نفوذ: یکی از روش‌های کاهش هشدارهای نادرست، ساخت حس‌گرهایی است که بتوانند نفوذها را با درصد کمتر تشخیص نادرست، کشف کنند. در شبکه‌های کامپیوتری می‌توان به جای به‌کارگیری موتورهای تشخیص[۱] با استفاده از تشخیص الگوی ساده، موتورهایی را استفاده کنیم که توانایی فهم پروتکل‌های قرار گرفته در زیرِ لایه انتقال را داشته باشند.
می‌توان به جای سیستم‌های تشخیص نفوذ همه‌جانبه به تمرکز بر روی موارد خاص، به عنوان مثال پروتکل‌های خاص و یا حملات خاص، پرداخت که در این صورت نرخ تشخیص نادرست کاهش می‌یابد. این خصوصی‌سازی سبب افزایش دقت سیستم‌های تشخیص نفوذ و بهبود کیفیت آن‌ها می‌گردد. با به‌کارگیری شبکه‌ای همسان از سیستم‌های تشخیص نفوذ، می‌توان کل حملات را تحت پوشش قرار داد.

ب. استفاده از اطلاعات محیط: از آن‌جایی که سیستم‌های تشخیص نفوذ دید محدودی از محیط دارند، در موارد بسیاری نمی‌توانند با قطعیت حملات را از غیر آن تشخیص دهند. استفاده از اطلاعات محیط با استفاده از پویش‌گرهای[۲] تشخیص آسیب‌پذیری و یا اطلاعات سیستم‌عامل نصب شده و موارد مشابه سبب می‌گردد تا محیط را بهتر شناسایی کنند و نرخ تشخیص نادرست آن‌ها پایین می‌آید.

ج. پردازش هشدار: در این روش پس از این‌که هشدارها توسط سیستم‌های تشخیص نفوذ ایجاد گردید، به تجزیه و تحلیل هشدارها و فیلتر کردن هشدارهای نادرست می‌پردازند و در مواقعی نیز کیفیت هشدارها را بالاتر می‌برند.

در این پایان‌نامه به حیطه‌ی کاری مورد «ج» پرداخته شده است که با بررسی و تحلیل هشدارها به کشف موارد نادرست و فیلتر کردن آن‌ها اقدام می‌گردد.

---

[۱] Detection Engine

[۲] Scanner

۴.۱ شرح موضوع پایان‌نامه

هدف از این پایان‌نامه کاهش هشدارهای نادرست در سیستم‌های تشخیص نفوذ توسط تحلیل هشدارهای تولیدشده می‌باشد. بدین منظور در صورت کشف هشدارهای نادرست، این هشدارها فیلتر گردیده و تنها هشدارهایی به تحلیل‌گر پیشنهاد داده می‌شود که با احتمال بالایی درست می‌باشند. در این راستا با استفاده از فرکانس خصوصیات هشدار به صورت بلادرنگ به کشف و فیلترینگ هشدارهای نادرست پرداخته می‌شود. اهداف اصلی انجام این پایان‌نامه به صورت زیر می‌باشد:

الف. طراحی روشی بلادرنگ که با عدم کاهش نرخ درست تشخیص، تا حد قابل قبولی تعداد هشدارهای نادرست را در سیستم‌های تشخیص نفوذ کاهش دهد.

ب. پیاده‌سازی روش پیشنهادی و تست آن با استفاده از مجموعه داده‌های موجود تا میزان کارآیی آن مشخص گردد.

محدوده‌ی کاری این پایان‌نامه معطوف به کاهش هشدارهای نادرست با استفاده از پردازش بر روی هشدارهای تولیدی سیستم‌های تشخیص نفوذ می‌گردد به صورتی که خللی بر میزان تشخیص درست سیستم وارد نیاید. نتیجه به دست آمده، سبب کاهش حجم کاری تحلیل‌گران هشدارها می‌شود. در این پایان‌نامه قصد نداریم کیفیت هشدارها را بالا ببریم و تنها به تشخیص و حذف هشدارهای نادرست با درجه اطمینان بالا و اعلام هشدارهای درست و یا مشکوک به تحلیل‌گر بسنده می‌نماییم.

در این پایان‌نامه بحثی در حیطه‌ی میزان تشخیص درست سیستم‌های تشخیص نفوذ صورت نمی‌گیرد. عدم توانایی تشخیص حملات و نفوذها در سیستم‌های تشخیص نفوذ خارج از حیطه‌ی این تحقیق می‌باشد و تنها هشدارهای تولید شده توسط سیستم مورد کاوش قرار می‌گیرند که تنها در صورت تشخیص حمله توسط سیستم ایجاد می‌گردند.

این پایان‌نامه برای آن دسته از پژوهشگرانی که بر روی موارد بالا بردن کیفیت هشدارها، همبستگی هشدارها، تشخیص سناریوی حمله و یا کشف مقصود مهاجم تحقیق می‌کنند می‌تواند مفید باشد و می‌توانند به عنوان پیش‌پردازش جهت کاهش حجم وسیع هشدارها از آن استفاده نمایند.

۵.۱ ساختار کلی پایان‌نامه

پایان‌نامه حاضر به صورت زیر سازماندهی شده است:

فصل ۲ به بررسی مختصر در زمینه کارهای صورت گرفته در زمینه کاهش هشدارهای نادرست به وسیله پردازش هشدارهای تولیدی سیستم‌های تشخیص نفوذ می‌پردازد.

فصل ۳ مفاهیم اصلی و اساسی امنیت و سیستم‌های تشخیص نفوذ مورد بررسی قرار می‌گیرد. سپس به طور جزئی‌تر به معرفی سیستم تشخیص نفوذ Snort پرداخته می‌شود که در آزمایشات این تحقیق از آن به عنوان معیار استفاده شده است .

فصل ۴ مجموعه داده‌های حملات موجود و مجموعه داده مورد استفاده را معرفی می‌گردد.

فصل ۵ روش پیشنهادی کاهش هشدارهای سیستم تشخیص نفوذ مورد بررسی قرار می‌گیرد.

فصل ۶ نتایج و آزمایشات روش پیشنهادی ارائه می‌گردد.

فصل ۷ نتایج کلی و پیشنهادات جهت بهبود بیشتر سیستم پیشنهادی ارائه می‌گردد.