ارائه یک روش همبسته سازی هشدارها به منظور تشخیص حملات کند

فرشید میری

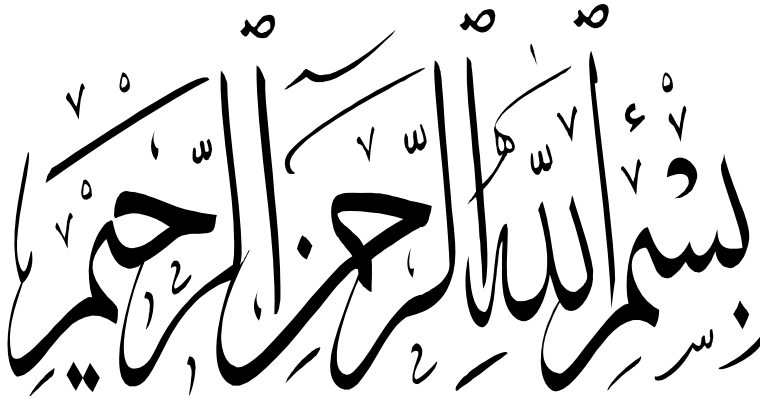
استاد راهنما:

جناب آقای دکتر محمدی

پایان نامه برای دریافت مدرک کارشناسی ارشد

رشته فناوری اطلاعات گرایش مدیریت سیستم‌های اطلاعات

شهریور ۹۲


بسم الله الرحمن الرحيم

تقدیم به مهربان فرشتگانی که؛

لحظات ناب باور بودن

لذت و غرور دانستن

جسارت خواستن

شکوه توانستن

عظمت رسیدن

و تمام تجربه‌های یکتا و زیبای زندگیم

مدیون حضور سبز آنهاست.

پدر و مادر عزیزم

تشکر و قدردانی:

وظیفه خود می‌دانم سپاسگزار تمام آنهایی باشم که در این دوره ارزشمند بودنشان و امیدشان راهگشای من بود؛ پدر ، مادر عزیزم که همانند تمام روزهای گذشته با صبر و حوصله در کنارم بودند.

اساتید عزیز و گرانقدر دانشکده مهندسی صنایع، بخصوص جناب آقای دکتر محمدی که با تلاش‌های بی‌شائبه خود نه‌تنها در انجام این سمینار بلکه در تمام دوره تحصیلم مرا یاری نمودند و به هنگام نیاز برای حل مشکلات اینجانب از هیچ کمکی دریغ نورزیدند. برای ایشان آرزوی سلامتی، موفقیت و سر بلندی را دارم.

چکیده

در حال حاضر مدیریت هشدارهای خام تولید شده توسط سنسورهای مختلف سیستم های تشخیص نفوذ که این سنسورها با قابلیت های مختلف در مکان های مختلف در شبکه قرار گرفته اند به مساله ای مهم تبدیل گردیده است .تمام سیستم های تشخیص نفوذ قادر به تولید هشدار در مورد وقوع نفوذ در شبکه می باشند ولی به علت حجم بالای هشدار های تولید شده توسط این سیستم ها و همچنین تولید هشدارهای اشتباه، این سیستم ها قادر به مدیریت و آنالیز هشدارهای تولید شده توسط خود نمی باشند. وجود این نقطه ضعف در این سیستم ها باعث ارائه روش های مختلفی برای رفع آن گردید که یکی از این روش ها همبسته سازی هشدارها می باشد. با استفاده از روش های همبسته سازی هشدارها می توان مدیریت کاملی بر روی هشدارهای تولید شده توسط سیستم های تشخیص نفوذ اعمال نمود. همچنین می توان تا اندازه زیادی با نادیده گرفتن هشدارهای اشتباه، حجم هشدارهای تولید شده توسط این سیستم ها را کاهش داد و آنالیز آنها را راحت تر نمود. در این گزارش به بررسی معماری ها و روش های موجود برای همبسته سازی هشدارها می پردازیم و در نهایت بیان می‌داریم که ترکیب روش‌های همبسته‌سازی می‌تواند ما را به هدفمان نزدیک کند.

کلمات کلیدی: امنیت شبکه، تشخیص نفوذ، هشدارهای درست و نادرست مثبت و منفی، همبسته سازی هشدارها، انواع حملات

فهرست مطالب

فهرست شکل‌ها و نمودارها

۲- فصل دوم: مفاهیم مقدماتی سیستمهای تشخیص نفوذ

۳- فصل ۳: مروری بر کارهای گذشته و معماری های موجود

٤- فصل ۴: انواع روشهای همبستگی

فهرست جداول

فصل اول

کلیات موضوع

۱- فصل اول: کلیات موضوع

۱-۱ هدف

با گسترش شبکه های کامپیوتری و افزایش روزافزون کاربران تحت این شبکه ها موضوع تامین امنیت در این شبکه ها به عنوان یکی از موضوعات باز در دنیای آکادمیک و دنیای تجاری مورد مطالعه محققین زیادی در سرتاسر دنیا قرار گرفته است .به همان میزانی که شبکه های کامپیوتری گسترش یافته اند میزان حملات خرابکارانه در این شبکه ها نیز افزایش یافته است به طوری که هر روزه شامل رخ دادن حملات زیاد و جدیدی در دنیای پیرامون خود می باشیم . برای برقراری امنیت از دستگاه های مختلفی در شبکه استفاده، می شود .این دستگاه ها به عنوان مثال شامل :سیستم های تشخیص نفوذ ، سیستم های جلوگیری از نفوذ، دیواره های آتش و ..... می باشند .ما در این تحقیق قصد داریم که بر روی سیستم های تشخیص نفوذ متمرکز گردیم .وظیفه اصلی سیستم های تشخیص نفوذ، تشخیص به موقع نفوذ یک نفوذگر به درون شبکه می باشد.

۱-۲ توضیح موضوع

با توجه به گستردگی شبکه های موجود و اینکه ممکن است در نقاط مختلفی از شبکه سنسورهای سیستم تشخیص نفوذ را نصب نموده باشیم، حجم هشدارهایی که توسط این این دستگاه ها تولید می شود بسیار زیاد خواهد بود .همچنین با توجه به اینکه عملکرد سیستم‌های تشخیص نفوذ یه صورت کامل درست نمی باشد ممکن است که در زمان تولید این هشدارها، هشدارهای اشتباهی تولید گردند که البته هشدارهای اشتباه انواع مختلفی دارند که در قسمت های بعدی گزارش به توضیح آنها خواهیم پرداخت .حال با توجه به حجم زیاد هشدارهای تولید شده توسط این سیستم ها و همچنین وجود هشدارهای اشتباه در میان هشدارهای درست مدیریت و بررسی این هشدارها توسط کاربر انسانی تقریبا غیر ممکن می باشد .روش های متعددی برای رفع این مشکل ارائه گردید که هریک مزایا و معایب خاص خود را داشتند اما یکی از این روش ها که در واقع شاید بتوان گفت بهترین روش می باشد، همبسته سازی هشدارها می باشد .منظور از همبسته سازی هشدارها این است که هشدارهای گوناگون و گاها مشابه که توسط سیستم های مختلف تشخیص نفوذ در شبکه تولید می گردد را با یکدیگر همبسته نمود) یعنی تعدادی از هشدارهای سطح پایین را با یکدیگر ترکیب نموده و باعث تولید یک هشدار سطح بالا گردیم (.که این کار باعث می شود که حجم هشدارها برای بررسی نسبت به حالت اولیه بسیار کاهش یابد .همچنین مزیت دیگر این کار این است که در طول همبسته سازی

هشدارها، می توان هشدارهای اشتباهی که توسط سیستم تولید گردیده است را شناسایی نموده و آنها را در طول همبسته سازی حذف نمود .مزیت دیگری که همبسته سازی هشدارها دارد این است که می توان پس از همبسته سازی هشدارهای سطح پایین با یکدیگر یک هشدار جدید تولید نموده که در سطحی انتزاعی تر و کاربردی تر و قابل فهم تر برای مدیر امنیت شبکه قرار داشته باشد همچنین می توان هشدارهای تولید شده پس از همبسته سازی را با توجه به حمله صورت گرفته و هشدار تولید شده اولویت دهی نمود که این کار باعث می شود که مدیر امنیت شبکه بتواند در مقابل حملات صورت گرفته عکس العمل مناسبی از خود نشان دهد و همچنین آسیب پذیری هایی که باعث وقوع آن حمله گردیده اند را ترمیم نماید.
به علت اهمیت زیاد مبحث همبسته سازی هشدارها در ادامه این گزارش به صورت متمرکز بر روی مبحث همبسته سازی هشدارها متمرکز می شویم .این گزارش به عنوان یک کار پژوهشی در رابطه با مبحث همبسته سازی هشدارها می باشد و هیچ گونه ایده جدیدی در آن وجود ندارد .

۱-۳ مرور کلی بر ادبیات موضوع

۱-۳-۱ تهدید[1]

افزایش نیاز به دسترسی به داده‌ها و پردازش سریعتر آن‌ها و در عین حال افزایش حجم داده‌ها و نیاز به فراهم آوردن داده‌ها از منابع مختلف از طریق شبکه‌های کامپیوتری، منجر به پدید آمدن منابع تهدید آمیزی می‌گردد که از طریق نقاط ضعف موجود در سیستم‌ها، به استثمار سیستم‌ها و ایجاد اختلال در آن‌ها می‌پردازد.

به طور کلی تهدید عبارت است از هر وضعیت یا اتفاقی که قابلیت ضرر زدن به سیستم را داشته باشد. این ضرر می‌تواند به صورت انکار، افشاء، خرابی یا تغییر داده‌ها و منابع سیستم باشد.

یک تهدید ممکن است از سوی منبعی انسانی باشد، مانند یک دسترسی غیر مجاز توسط یک

---

[1] Threat

فرد به اطلاعاتی خاص، یا از سوی منبعی فیزیکی، نظیر حوادثی چون سیل، آتش سوزی و قطع برق و یا از سوی منبعی کامپیوتری، مثل ویروس‌ها و حمله اسب‌های تروایی[۲]. تهدیدات می‌توانند داخلی باشند و یا خارجی و همچنین می‌توانند عمدی باشند یا غیر عمدی.

جیمز اندرسون تهدیدات کامپیوتری را به شکل زیر دسته بندی کرده است :

۱. رخنه گران[۳] خارجی : کسانی که مجاز به استفاده از کامپیوتر مربوطه نیستند.
۲. رخنه گران داخلی : کسانی که مجاز به استفاده از کامپیوتر هستند اما حق استفاده از داده‌های خاصی را ندارند.

تهدیدات داخلی خود به سه دسته تقسیم می‌گردند :

۱. نقاب داران[۴] : آن‌هایی که با سرقت هویت و اعتبار دیگران وارد سیستم می‌گردند.
۲. .کاربران نا مشروع[۵] : آن‌هایی که به طور موفق از معیارهای نظارت و ممیزی عبور می‌کنند.
۳. سوء استفاده گرها[۶] : کسانی که هم حق استفاده از کامپیوتر و هم حق استفاده از داده‌ها را دارند اما از حقوق خود سوء استفاده می‌کنند.

برای حفاظت سیستم و به خصوص اطلاعات حساس آن از تهدیدات فوق، سرویس‌های زیر ضروری هستند :

---

[2] Trojan Horses Attack

[3] Penetrator

[4] Masqueraders

[5] Clandestine Users

[6] Misfeasor

۱. هویت شناسی[۷] و احراز اصالت[۸] : سیستم را قادر به تشخیص هویت کاربران آن می‌نماید.

۲. کنترل دسترسی[۹] : درخواست کاربران مجاز را در دسترسی به منابع، بر اساس یک سری قوانین دستیابی، مورد بررسی قرار داده و مشخص می‌نماید که مجاز به این دسترسی هستند یا خیر.

۳. ممیزی[۱۰] : یک ارزیابی و بررسی، پس از درخواست و دسترسی به سیستم است، برای تشخیص اینکه تجاوزی رخ داده است و یا نه و یا اینکه تلاشی برای این منظور انجام پذیرفته است یا نه.

۴. رمزگذاری[۱۱] : این اطمینان را می‌دهد که هر داده‌ای که در سیستم ذخیره شده و یا بر روی شبکه ارسال می‌گردد، تنها توسط گیرنده مورد نظر رمزگشایی شده و مورد استفاده قرار گیرد.

۱-۳-۲ نفوذ

به هر مجموعه از اعمال که هدف آن نقض جامعیت، محرمانگی یا دسترس پذیری یک منبع باشد، نفوذ[۱۲] گفته می‌شود.

این تعریف تمام انواع تهدیدات را در بر می‌گیرد. تعریف دیگری که از نفوذ ارائه شده عبارت

---

[7] Identification

[8] Authentication

[9] Access Control

[10] Audit

[11] Encryption

[12] Intrusion

است از یک دسترسی غیرمجاز و یا فعالیتی علیه یک سیستم اطلاعاتی / ارتباطی، چه به صورت سهوی و چه به صورت عمدی.

۱-۳-۳ نفوذ گر

نفوذ گر[۱۳]، به فرد، گروه، سازمان یا وضعیتی گفته می‌شود که مسئول یک نفوذ است و یا به عبارت دیگر قصد نقض کردن ویژگی‌های امنیتی یک سیستم کامپیوتری را دارد. نفوذ گر معمولاً از راه‌های زیر برای رسیدن به مقصد خود استفاده می‌کند :

۱. وقفه[۱۴] : برای خراب کردن، غیرقابل دسترس کردن یا غیرقابل استفاده کردن یک سیستم استفاده می‌شود. نتیجه‌ی آن نقض دسترس پذیری است.
۲. حائل شدن[۱۵] : برای کسب دسترسی غیرمجاز به داده‌ها انجام شده و نتیجه‌ی آن نقض محرمانگی است.
۳. تغییر : برای ایجاد تغییر در سیستم انجام می‌گیرد. مانند تغییر پیام‌های فرستاده شده از یک سیستم به سیستم دیگر. نتیجه‌ی این کار نقض جامعیت است.

۱-۳-۴ تهاجم، مهاجم و مدافع

به یک نفوذ عمدی در یک سیستم اطلاعاتی / ارتباطی، تهاجم[۱۶] گفته می‌شود و به فرد، گروه، سازمان و یا وضعیتی که یک تهاجم را انجام می‌دهد، مهاجم[۱۷] گویند.

---

[13] Intruder

[14] Interruption

[15] Interception

[16] Attack

[17] Attacker

در تعریف ارائه شده از تهاجم باید به عمدی بودن آن توجه داشت، چرا که وجه تمایز بین تهاجم و نفوذ و تهدید، در عمدی بودن تهاجم است، چرا که نفوذ و تهدید هر دو می‌توانند به صورت غیر عمدی نیز صورت پذیرند.

بدین ترتیب به فرد، گروه یا سازمانی که مسئول سیستم اطلاعاتی / ارتباطی (مورد هدف) می‌باشد، مدافع[۱۸] گویند.

۱-۳-۵ وصله امنیتی(راهکار اصلاحی)[۱۹]

وصله های امنیتی راهکاری برای حذف آسیب پذیری های موجود در سیستم هستند که با به روز رسانی سرویس یا انجام کنترل دسترسی بر روی آن، امکان نفوذ به سرویس مربوطه را کاهش می دهند.

۱-۳-۶ امنیت

امنیت[۲۰]، یکی از مهم‌ترین چالش‌هایی است که سازمان‌ها و شرکت‌های استفاده کننده از شبکه با آن روبرو می‌باشند. سیستم‌های تشخیص نفوذ، یکی از راهکارهای موجود برای نظارت بر وضعیت امنیتی شبکه‌ها و تحلیل آن‌ها می‌باشند.

این سیستم‌ها با کنترل بسته‌های ارسالی بر روی شبکه، در صورت بروز ناهنجاری، هشدار های متناسب با مشکل تشخیص داده شده صادر می‌کنند .متأسفانه تعداد این هشدارها آنقدر زیاد و سطح انتزاع آن‌ها آنقدر پایین می‌باشد که تحلیل آن‌ها در عمل برای مدیر شبکه امکان پذیر نمی‌باشد .پژوهشگران تلاش کرده‌اند تا به کمک رویکردهای مبتنی بر قانون، مبتنی بر سناریو،

---

18 Defender

19 Security Patch

20 Security

آماری و زمانی، این هشدارها را با یکدیگر همبسته کنند.

در شبکه کامپیوتری برای کاهش پیچیدگی‌های پیاده سازی، آن را مدل سازی می‌کنند که از جمله می‌توان به مدل هفت لایه[۲۱] و مدل چهار لایه اشاره نمود. در این مدل‌ها، شبکه لایه بندی شده و هر لایه با استفاده از پروتکل‌های خاصی به ارائه خدمات مشخصی می‌پردازد. مدل چهار لایه[۲۲] نسبت به هفت لایه محبوبیت بیشتری پیدا کرده است ولی علیرغم این محبوبیت دارای نقاط ضعف و اشکالات امنیتی است که باید راهکارهای مناسبی برای آن‌ها ارائه شود تا نفوذ گران نتوانند به منابع شبکه دسترسی پیدا کرده و یا اینکه اطلاعات را بربایند. (اسکارفون[۲۳] و همکاران،۲۰۰۷)

شناسائی لایه‌های مدلTcp/ip ، وظایف، پروتکل‌ها و نقاط ضعف و راهکارهای امنیتی لایه‌ها در تعیین سیاست امنیتی مفید است اما نکته‌ای که مطرح است اینست که تنوع شبکه‌های کامپیوتری از نظر معماری، منابع، خدمات، کاربران و مواردی از این دست، ایجاد سیاست امنیتی واحدی را برای شبکه‌ها غیرممکن ساخته و پیشرفت فناوری نیز به این موضوع دامن میزند و با تغییر داده‌ها و تجهیزات نفوذ گری، راهکارها و تجهیزات مقابله با نفوذ نیز باید تغییر کند. سطح شبکه در مدل امنیت لایه بندی شده به WAN و LAN داخلی اشاره دارد. شبکه داخلی ممکن است شامل چند کامپیوتر و سرور و یا پیچیده‌تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه‌های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می‌توانید به راحتی در میان شبکه حرکت کنید.

که به این ترتیب این شبکه‌ها برای هکرها و افراد بداندیش به اهدافی وسوسه انگیز مبدل

---

[21] Osi

[22] Tcp/ip

[23] K.Scarfone et al.