
بسم الله الرحمن الرحيم
الحمد لله رب العالمين الرحمن الرحيم
اهدنا الصراط المستقيم غير المغضوب عليهم

دانشگاه شهید بهشتی
دانشکده مهندسی برق و کامپیوتر

سیستم تشخیص نفوذ با بکارگیری همبستگی بین هشدارها

پایان نامه کارشناسی ارشد مهندسی کامپیوتر
گرایش نرم افزار

توسط:
حامد موسوی

استاد راهنما:
دکتر عباسپور

۱۳۸۸

دانشگاه شهید بهشتی

دانشکده مهندسی برق و کامپیوتر

پایان نامه کارشناسی ارشد مهندسی کامپیوتر- گرایش نرم افزار

تحت عنوان:

سیستم تشخیص نفوذ با بکارگیری همبستگی بین هشدارها

در تاریخ ۱۳۸۸/۰۶/۲۴ پایان نامه دانشجو، (حامد موسوی)، توسط کمیته تخصصی داوران مورد بررسی و تصویب نهائی قرار گرفت.

۱- استاد راهنما اول:	دکتر مقصود عباسپور	امضاء
۲- استاد داور (داخلی)	دکتر فرشاد صفایی	امضاء
۳- استاد داور (خارجی)	دکتر مهدی خرازی	امضاء
۴- نماینده تحصیلات تکمیلی	دکتر فرح ترکمنی آذر	امضاء

پیشگفتار، تقدیر و تشکر

به نام خداوندی که طلوع کلام علم را با قلم آغاز نمود
"من لم یشکر المخلوق لم یشکر الخالق"

رسیدن این پژوهش به منزلگه حاضر مرا وامدار فرهیختگانی ساخت، که سال‌ها لحظه لحظه‌ی عمر خویش را در قلم افشردند و به اندیشه‌ها حیات، به روح کمال و به جان جمال بخشیدند. در این منزلگه شایسته است از اساتید فرزانه‌ام جناب آقای دکتر مقصود عباسپور، استاد محترم دانشگاه شهید بهشتی تشکر و قدردانی نمایم که عطش نوجویی جان مرا در پی یافتن چشمه‌های علم و دانش سیراب ساختند و بالندگی علمی خویش را وامدار ایشان می‌باشم.

از داوران محترم جناب آقای دکترخرازی استاد محترم دانشگاه شریف و به خصوص جناب آقای دکتر صفایی استاد محترم دانشگاه شهید بهشتی که در گردآوری نهایی این پایان نامه نیز مرا یاری رساندند کمال تشکر را دارم. بزرگوارانی که مرا در علم و تجربه خویش شریک ساختند و با صبر و حوصله مرا یاری رساندند.

همچنین از دوستان عزیز آقای مرتضی دامن افشان که دانش من در این پروژه ناشی از همکاری پیشین با این دوست عزیز است و دوست عزیز دیگر آقای اسماعیل دوست که بخشی از پروژه با همکاری ایشان صورت گرفت، نهایت سپاسگذاری را دارم. و نهایتا از جناب آقای مهندس بهزادی مدیر وقت مرکز تحقیقات فیزیک نظری بخش شبکه (اختیاریه) که با فراهم نمودن محیط مناسب جهت تحقیقات اینجانب، لطف بیشماری به بنده ابراز داشتند نیز کمال تشکر را دارم.

کلیه حقوق مادی مترتب بر نتایج مطالعات،

ابتکارات و نوآوریهای ناشی از تحقیق موضوع

این پایان نامه متعلق به دانشگاه شهید بهشتی

می باشد.

به نام خدا

نام ونام خانوادگی: حامد موسوی

عنوان پایان نامه: سیستم تشخیص نفوذ با بکارگیری همبستگی بین هشدارها

استاد/اساتید راهنما: دکتر مقصود عباسپور

نام ونام خانوادگی دانشجو: حامد موسوی

امضاء و تاریخ:

فهرست مطالب

چکیده

امروزه سیستم های تشخیص نفوذ به طور قابل ملاحظه ای برای افزایش امنیت شبکه های کامپیوتری مورد استفاده قرار می گیرند. حجم بالا و کیفیت پایین هشدارهای تولید شده، نیاز به پردازش بیشتر این هشدارها را توجیه می کند. در این راستا، روش های همبسته سازی هشدارها با هدف افزایش کیفیت هشدارها و ارایه جمع بندی قابل درک از وضعیت امنیتی جاری به تحلیلگر امنیتی مطرح شده اند. در این پایان نامه با ترکیب دو روش خوشه بندی هشدارها و کشف اپیزودهای تکرارشونده در دنباله هشدارها نتایج جالبی روی داده های DARPA بدست آمده است. این روش هم می تواند به عنوان یک سیستم نظارتی که نقاط ضعف شبکه را شناسایی نماید عمل کند و هم می تواند بخش مهمی از سناریو حمله را شناسایی کند. مزیت این روش عدم نیاز به اطلاعات از پیش تعریف شده و توانایی شناسایی حملات جدید می باشد. از طرف دیگر این روش دارای نرخ مثبت و منفی نادرست است.

کلمات کلیدی

همبسته سازی هشدارها، تشخیص نفوذ

فصل اول

مقدمه

در سال های اخیر، استفاده از سیستم های تشخیص نفوذ[1] به طور گسترده ای مورد توجه قرار گرفته است. این سیستم ها، وقوع حملات را تشخیص داده و هشدارهایی[2] تولید می کنند. مدیران سیستم و یا سیستم های پاسخ به نفوذ[3] با استفاده از هشدارهای تولید شده، وضعیت فعلی را ارزیابی کرده و واکنش های لازم را نشان می دهند.

سیستم های تشخیص نفوذ، از جهت نحوه تشخیص به دو دسته تقسیم می شوند: سیستم های تشخیص ناهنجاری (رفتار غیر عادی[4]) و سیستم های سوء استفاده[5]. سیستم های تشخیص ناهنجاری (رفتار غیرعادی) از توصیف رفتار عادی کاربران یا برنامه های کاربردی استفاده می کنند و رفتارهایی را که در این توصیف نگنجد، به عنوان حمله تلقی کرده و هشدار تولید می کنند. در مقابل، سیستم های تشخیص سوء استفاده امضای حملات را دریافت می کنند و رفتارهایی را که با این امضاء مطابقت داشته باشند، به عنوان حمله تشخیص می دهند.

سیستم های تشخیص ناهنجاری، به علت تنوع رفتار عادی کاربران دارای نرخ بالای مثبت (اعلام) نادرست[6] هستند. در مقابل، دارای قابلیت تشخیص حملات جدید (ناشناخته) هستند. سیستم های تشخیص سوء استفاده، تنها حملاتی را تشخیص می دهند که قبلا شناخته شده اند و توصیف آنها مشخص است. به همین دلیل ، دارای نرخ بالای منفی نادرست[7] هستند.

---

[1] IDS : Intrusion Detection System

[2] Alert

[3] IRS : Intrusion Response System

[4] Anomaly Detection

[5] Misuse Detection

[6] False Positive

[7] False Negative

سیستم های تشخیص نفوذ از جهت دامنه عملیاتی نیز به دو دسته تقسیم می شوند: سیستم های مبتنی بر میزبان[1] و سیستم های مبتنی بر شبکه[2]. سیستم های مبتنی بر میزبان، حملات محلی یک میزبان را با استفاده از اطلاعات سیستم عامل یا برنامه های کاربردی تشخیص می دهند. از سوی دیگر، سیستم های مبتنی بر شبکه حملات را با توجه به بسته های مبادله شده در شبکه تشخیص می دهند. اطلاعات تشخیص داده شده توسط سیستم های مبتنی بر میزبان و سیستم های مبتنی بر شبکه ، مکمل یکدیگر هستند. اطلاعاتی نظیر پردازه و کاربر توسط سیستم های مبتنی بر میزبان و اطلاعاتی نظیر مبدأ، مقصد و پروتکل توسط سیستم های مبتنی بر شبکه تشخیص داده می شوند.

معمولا مهاجمین، حملات را یکی پس از دیگری برای رسیدن به هدف مشخصی انجام می دهند. به طوری که حمله قبلی، مقدمه حمله بعدی را فراهم می کند. همبسته سازی هشدارها[3] به عنوان رویکردی برای پردازش هشدارهای تولید تولید شده توسط سیستم های تشخیص نفوذ مورد توجه قرار گرفته است. هدف از همبسته سازی، ارائه دورنمایی جامع از اتفاقات رخ داده در سیستم به مدیر سیستم یا سیستم پاسخ به نفوذ است.

با توجه به حجم بالای هشدارهای تولید شده توسط سیستم های مختلف تشخیص نفوذ، همپوشانی بعضی هشدارها، و وجود مثبت (اعلام) نادرست و منفی نادرست در سیستم های تشخیص نفوذ مختلف، به همبسته سازی هشدارهای تشخیص نفوذ نیازمندیم. روش های همبسته سازی تلاش می کنند با تشخیص سناریوی حملات، کاهش هشدارهای مثبت (اعلام) نادرست، حدس حملات تشخیص داده نشده، تشخیص استراتژی حمله و پیش بینی گام (های) بعدی حمله، کیفیت هشدارها را افزایش داده و اطلاعات دقیق تر و کامل تری را ارائه دهند.

در این پایان نامه، ابتدا روشها و الگوریتم های مختلف در زمینه همبسته سازی هشدارها به طور مختصر مورد مطالعه و بررسی قرار گرفته و سپس راه حلی جدید در این زمینه همراه با نتایج آن ارایه گردیده است. در ادامه این پایان نامه، در فصل ۲ با مفاهیم پایه مورد نیاز آشنا می شویم. در فصل ۳ مروری بر کارهای انجام شده در زمینه همبسته سازی هشدارها خواهیم داشت. در فصل۴ طرح اصلی پایان نامه مورد بررسی قرار می گیرد. در فصل ۵ شبیه سازی و نتایج آورده شده است.در فصل۶ راه حل سخت افزاری جهت افزایش کارایی ارایه شده و نهایتا در پایان نتیجه گیری قرار دارد.

---

[1] Host - based

[2] Network - based

[3] Alert Correlation

فصل دوم

مفاهیم پایه

دراین فصل، مفاهیم و تعاریف مورد استفاده در زمینه امنیت کامپیوتری و در چارچوب همبسته سازی هشدارها معرفی شده است. حال تعاریف پایه در زمینه امنیت کامپیوتری را مرور می کنیم.

۲-۱ تعاریف پایه در امنیت کامپیوتری

۲-۱-۱ تهدید

افزایش نیاز به دسترسی به داده ها و پردازش سریع تر آن ها و در عین حال افزایش حجم داده ها و نیاز به فراهم آوردن داده ها از منابع مختلف از طریق شبکه های کامپیوتری، منجر به پدید آمدن منابع تهدید آمیزی گردید که از طریق نقاط ضعف موجود در سیستم ها ، به استثمار سیستم ها و ایجاد اختلال در آن ها می پردازند[۱۳].

به طور کلی، تهدید[1] عبارت است از هر وضعیت یا اتفاقی که قابلیت ضرر زدن به سیستم را داشته باشند[۲]. این ضرر می تواند به صورت انکار، افشاء خرابی یا تغییر داده ها و منابع سیستم باشد.

یک تهدید ممکن است از سوی منبعی انسانی باشد، مانند یک دسترسی غیر مجاز توسط یک 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 ویروس ها و حمله اسب های تروایی [2][۱۳]. تهدیدات می توانند داخلی باشند ویا خارجی و همچنین می توانند عمدی باشند ویا غیر عمدی.

جیمز اندرسون تهدیدات کامپیوتری را به شکل زیر دسته بندی کرده است[۲]:

۱. رخته گران[3] خارجی : کسانی که مجاز به استفاده از کامپیوتر مربوطه نیستند.

---

[1] Threat

[2] Trojan Horses Attack

[3] Penetrator

۲. رخنه گران داخلی : کسانی که مجاز به استفاده از کامپیوتر هستند اما حق استفاده از داده های خاصی را ندارند.

تهدیدات داخلی خود به دو دسته تقسیم می گردند :

- نقابداران [1]: آنهایی که با سرقت هویت و اعتبار دیگران وارد سیستم می گردند.
- کاربران نهان [2] : آنهایی که به طور موفق از معیارهای نظارت و ممیزی عبور می کنند.

۳. سوء استفاده چی ها [3]: کسانی که هم حق استفاده از کامپیوتر و هم حق استفاده از داده ها را دارند اما از حقوق خود سوء استفاده می کنند.

برای حفاظت سیستم و به خصوص اطلاعات حساس آن از تهدیدات فوق، سرویس های زیر ضروری هستند. [۲۱] :

۱. هویت شناسی [4] و احراز هویت [5] : سیستم را قادر به تشخیص هویت کاربران آن می نماید.

۲. کنترل دسترسی [6] : درخواست کاربران مجاز را در دسترسی به منابع، براساس یک سری قوانین دستیابی، مورد بررسی قرار داده و مشخص می نماید که مجاز به این دسترسی هستند یا خیر.

۳. ممیزی [7] : یک ارزیابی و بررسی، پس از درخواست و دسترسی به سیستم است، برای تشخیص اینکه تجاوزی رخ رخ داده است یا نه و یا اینکه تلاشی برای این منظور انجام پذیرفته است یا نه .

۴. رمز نگاری [8] : این اطمینان را می دهد که هر داده ای که در سیستم ذخیره شده ویا برروی شبکه ارسال می گردد، تنها توسط گیرنده مورد نظر رمز گشایی شده و مورد استفاده قرار گیرد.

---

1 Masqueraders

2 Clandestine Users

3 Misfeasor

4 Identification

5 Authentication

6 Access Control

7 Audit

8 Encryption

۲-۱-۲ آسیب پذیری

آسیب پذیری[1] عبارت است از ضعف در رویه های امنیتی خودکار، رویه های مدیریتی[2] ویا رویه های کنترلی داخلی که به وسیله یک تهدید در جهت دسترسی غیر مجاز به اطلاعات ویا از هم گسیختگی (یا انقطاع) در یک پردازش حساس و حیاتی، مورد بهره برداری و استثمار قرار می گیرد. به نقاط آسیب پذیری یک سیستم حفره امنیتی[3] سیستم نیز گویند. گویند.

جیمز اندرسون یک آسیب پذیری را با سطح انتزاعی پایین تر بدین صورت تعریف می نماید که آسیب پذیری عبارت است از درز یا رخنه شناخته شده و یا مشکوک در طراحی یا عملکرد سخت افزار یا نرم افزار یک سیستم که موجب نفوذ در اطلاعات آن سیستم می گردد[۱۳].

ضعف ها و نقاط آسیب پذیری سیستم ها را می توان به طور کلی به دو دسته زیر تقسیم نمود:

- ضعف در طراحی وپیاده سازی نرم افزار یا سخت افزار سیستم، که به حفره های فنی سیستم معروفند.
- ضعف در سیاست امنیتی ، پیکربندی، کنترل یا مدیریت سیستم ،که به آنها حفره های مدیریتی گویند.

باید توجه داشت که تهدید و آسیب پذیری ذاتا با یکدیگر در ارتباطند، چرا که تهدید ، نتیجه سوء استفاده از یک یا چند حفره امنیتی یا نقاط آسیب پذیری در یک سیستم می باشد.

۲- ۱- ۳ نفوذ

به هر مجموعه از اعمال که هدف آن نقض جامعیت، محرمانگی یا دسترس پذیری یک منبع باشد نفوذ[4] گفته می شود. این تعریف تمام انواع تهدیدات را دربرمی گیرد. تعریف دیگری که از نفوذ ارائه شده عبارت است از یک دسترسی غیر مجاز ویا فعالیتی علیه یک سیستم اطلاعاتی/ ارتباطی، چه به صورت سهوی وچه به صورت عمدی[۵].

---

[1] Vulnerability

[2] Administrative

[3] Security Hole

[4] Intrusion

۲-۱-۴ نفوذگر

اخلال گر[1]،به فرد، گروه، سازمان یا وضعیتی گفته می شود که مسوول یک نفوذ است[۵] ویا به عبارت دیگر قصد نقض کردن ویژگی های امنیتی یک سیستم کامپیوتری را دارد. نفوذگر معمولا از راه های زیر برای رسیدن به قصد خود استفاده می کند:

- وقفه [2]: برای خراب کردن، غیر قابل دسترس کردن یا غیر قابل استفاده کردن یک سیستم استفاده می شود. نتیجه آن نقض دسترس پذیری است.
- استراق سمع [3]: برای کسب دسترسی غیرمجاز به داده ها انجام شده و نتیجه آن نقض محرمانگی است.
- تغییر : برای ایجاد تغییر در سیستم انجام می گیرد. مانند تغییر پیام های فرستاده شده از یک سیستم به سیستم دیگر. نتیجه این کار نقض جامعیت است.

۲-۱-۵ تهاجم ، مهاجم و مدافع

به یک نفوذ عمدی در یک سیستم اطلاعاتی/ ارتباطی ، تهاجم[4] گفته می شود وبه فرد، گروه، سازمان ویا وضعیتی که یک تهاجم را انجام می دهد، مهاجم[5] گویند[۵].

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 می باشد، چرا که نفوذ و تهدید هر دو می توانند به صورت غیر عمدی نیز صورت پذیرند.

بدین ترتیب به فرد، گروه یا سازمانی که مسوول سیستم اطلاعاتی/ ارتباطی (مورد هدف) می باشد، مدافع [6]گویند.[۵]

۲-۱-۶ تشخیص نفوذ

---

[1] Intruder

[2] Interruption

[3] Interception

[4] Attack

[5] Attacker

[6] Defender

تشخیص نفوذ[1] فرآیند نظارت بر وقایع رخ داده در یک شبکه ویا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاست های امنیتی است [۲]. یک سیستم تشخیص نفوذ (IDS) ، طبق تعریف ارائه شده توسط دنینگ در سال ۱۹۸۷ عبارت است از یک نرم افزار با قابلیت تشخیص، آشکار سازی و پاسخ به فعالیت های غیر مجاز یا غیر نرمال در رابطه با سیستم. وجود سیستم های تشخیص نفوذ از آن جهت اهمیت دارد که با وجود تمام مکانیزم های امنیتی از جمله اعتبار سنجی و هویت شناسی، رمزگذاری و رمزگشایی، حفاظ[2] (دیوار آتش)، کنترل دسترسی وغیره، باز هم یک سیستم دارای نقاط آسیب پذیری زیادی است که امکان بروز حمله از این نقاط به سیستم وجود دارد. پس بدین ترتیب ایجاد یک سیستم کاملا امن بسیار مشکل و تقریبا غیر ممکن است و حتی اگر سیستمی تولید گردد که ادعای امنیت کامل را نماید باز هم با وجود سوء استفاده ها و حملات داخلی، ادعایش رد می شود. پس با این وجود باید از ابزاری جهت کشف نفوذات رخ داده در یک سیستم جهت پاسخگویی و بروز عکس العمل مناسب در مقابل آنها و پیشگیری از حملات بعدی استفاده نمود، که این ابزار، همان سیستم های تشخیص نفوذ می باشند.

هر سیستم تشخیص نفوذ حداقل دارای سه مولفه اصلی زیر می باشد[۲]:

۱. یک منبع اطلاعات که جریانی از رکوردهای وقایع (وقایع رخ داده در سیستم یا شبکه) را فراهم می آورد.
۲. یک موتور تحلیل که الگوهای نفوذ را تشخیص می دهد.
۳. یک مولفه پاسخگویی که براساس خروجی های حاصل از موتور تحلیل عکس العمل مناسب را از خود نشان می دهد.

۲-۱-۷ دسته بندی سیستم های تشخیص نفوذ

سیستم های تشخیص نفوذ از دو جهت دسته بندی می شوند:

۱. نحوه تشخیص: سیستم های تشخیص نفوذ از جهت نحوه تشخیص به دو دسته کلی تقسیم می شوند: سیستم های تشخیص ناهنجاری و سیستم های تشخیص سوء استفاده. سیستم های تشخیص ناهنجاری(رفتار غیر عادی) از توصیف رفتار عادی کاربران و برنامه ها استفاده می کنند و رفتارهایی را که در این توصیف نگنجد، به

[1] Intrusion Detection

[2] Firewall

عنوان حمله تلقی کرده و هشدار تولید می کنند. در مقابل، سیستم های تشخیص سوء استفاده، امضای حملات را دریافت می کنند و رفتارهایی را که با این امضا مطابقت داشته باشند، به عنوان حمله تشخیص می دهند. سیستم های تشخیص ناهنجاری، به علت تنوع رفتار عادی کاربران دارای نرخ بالای مثبت (اعلام) نادرست هستند . یعنی با نرخ بالایی رفتارغیر نفوذی[1] را به عنوان حمله تشخیص می دهند. در مقابل، دارای قابلیت تشخیص حملات جدید (ناشناخته) هستند. سیستم های تشخیص سوء استفاده، تنها حملاتی را تشخیص می دهند که قبلا شناخته شده اند و توصیف آنها مشخص است. به همین دلیل، دارای نرخ بالای منفی نادرست هستند. یعنی ممکن است حملات واقعی را به عنوان رفتار غیر نفوذی در نظر بگیرند.

۲. دامنه عملیاتی : سیستم های تشخیص نفوذ از جهت دامنه عملیاتی نیز به دو دسته تقسیم می شوند: سیستم های مبتنی بر میزبان و سیستم های مبتنی بر شبکه[2]. سیستم های مبتنی بر میزبان،حملات محلی یک میزبان را با استفاده از اطلاعات سیستم عامل یا برنامه های کاربردی تشخیص می دهند. از سوی دیگر، سیستم های مبتنی بر شبکه حملات را با توجه به بسته های مبادله شده در شبکه تشخیص می دهند. اطلاعات تشخیص داده شده توسط سیستم های مبتنی بر میزبان و سیستم های مبتنی بر شبکه، مکمل یکدیگر هستند. اطلاعاتی نظیر پردازه و کاربر توسط سیستم های مبتنی بر میزبان و اطلاعاتی نظیر مبدا، مقصد و پروتکل توسط سیستم های مبتنی بر شبکه تشخیص داده می شوند.

---

[1] Non – intrusive

[2] Network – based

فصل سوم

کارهای انجام شده

در این فصل، کارهای انجام شده در زمینه همبسته سازی ارائه شده اند. ابتدا نگاهی به تعریف فرآیند همبسته سازی خواهیم داشت. سپس به بررسی روش های احتمالاتی، مبتنی بر تشخیص سناریو، مبتنی بر روابط پیش نیازی و مبتنی بر گراف حمله خواهیم داشت. در انتها، روش هایی را که از شبکه علی برای استنتاج احتمالاتی استفاده کرده اند، بررسی خواهیم نمود.

۳-۱ رویکرد جامع به همبسته سازی

همبسته سازی هشدارها، مفهومی است که منابع مختلف به ضرورت آن اشاره کرده اند. اما تعریف مشترک و واحدی از آن وجود ندارد. والور[1] و همکاران [۲۵] با رویکردی جامع همبسته سازی را به عنوان یک فرآیند مشتمل بر چندین مولفه[2]تعریف کرده اند. طبق این تعریف ، " همبسته سازی هشدارها یک فرآیند تحلیلی است که به عنوان ورودی هشدارهای تولید شده توسط سیستم های تشخیص نفوذ را دریافت می کند و گزارش های فشرده ای از وضعیت امنیتی شبکه تحت نظارت ارائه می دهد." اگر چه چندین رویکرد همبسته سازی ارائه شده است، اجماعی در مورد ماهیت فرآیند همبسته سازی و اجزای آن وجود ندارد. بعضی از روش های همبسته سازی ارائه شده، تنها به جنبه هایی از این فرآیند، نظیر ادغام هشدارهای تولید شده، یا تشخیص حملات چند مرحله ای پرداخته اند. همین ابهام در مورد نحوه ارزیابی این فرآیند نیز وجود دارد. معمولا فرآیندهای همبسته سازی ارائه شده به طور یکپارچه ارزیابی شده اند، بدون آنکه اثر بخشی[3] هر یک از مولفه ها به طور جداگانه مورد بررسی قرار گرفته باشد.

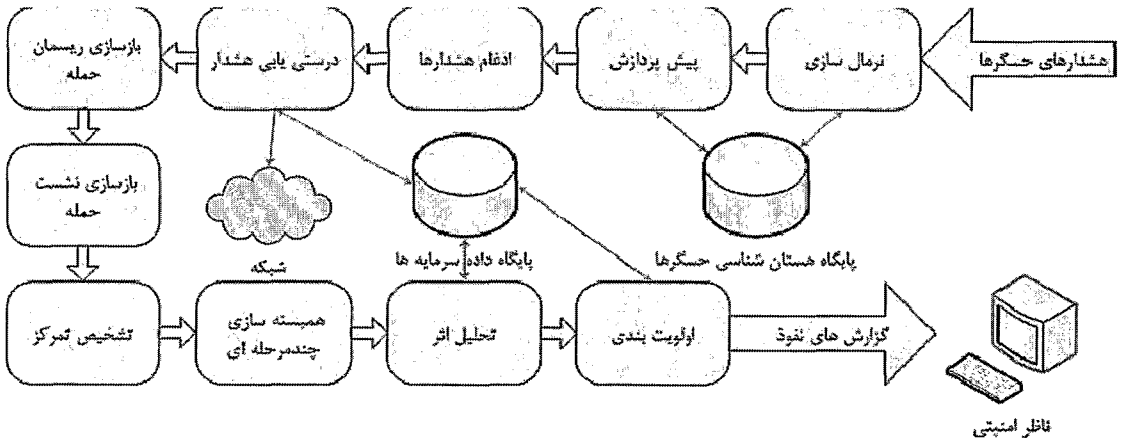
---

[1] Valeur

[2] Component

[3] Effectiveness

فرآیند همبسته سازی به عنوان فرآیندی شامل چندین مولفه ارائه شده است که هشدارهای سیستم های تشخیص نفوذ را به گزارش نفوذ تبدیل می کند. هر یک از مولفه ها بر جنبه های متفاوتی از عمل همبسته



شکل ۳-۱ رویکرد جامع به همبسته سازی [۲۵]

سازی تمرکز دارند. بعضی مولفه ها می توانند بر روی همه هشدارها، مستقل از نوعشان عمل کنند. این مولفه ها در ابتدا و انتهای فرآیند همبسته سازی، مورد استفاده قرار می گیرند. بقیه مولفه ها، تنها برای نوع خاصی از هشدارها کاربرد دارند. این مولفه ها، مسئول عملکردهایی هستند که قابل تعمیم به همه هشدارها نیستند.

فرآیند همبسته سازی در شکل ۳-۱ نمایش داده شده است. فرایند با مولفه های[1] نرمال سازی و پیش پردازش[2]، آغاز می شود. بعد از مولفه های نرمال سازی و پیش پردازش که روی همه هشدارها عمل می کنند، مولفه هایی در هسته فرآیند قرار دارند که روی ویژگی های زمانی و فضایی[3] متفاوتی عمل می کنند. بعضی از این مولفه ها، رخدادهایی را همبسته می کنند که از نظر زمانی و فضایی به هم نزدیک هستند، نظیر هشدارهای تولید شده روی یک میزبان در یک فاصله زمانی کوتاه. بعضی دیگر، روی رخدادهایی عمل می کنند که یک سناریوی حمله را دربرمی گیرند که ممکن است طی چند ساعت رخ دهد و شامل هشدارهای تولید شده روی چند میزبان باشد.

---

[1] Normalization

[2] Pre-process

[3] Spatial

چهار مولفه همبسته سازی بعدی، همگی روی یک هشدار و یا هشدارهای نزدیک به هم عمل می کنند. این مولفه ها شامل مولفه ادغام[۱] ، مولفه درستی یابی[۲] ، مولفه بازسازی ریسمان [۳]حمله و مولفه بازسازی نشست[۴] حمله هستند. دو مولفه بعدی، می توانند شامل تعداد زیادی میزبان باشند. این دو مولفه، شامل تشخیص تمرکز و همبسته سازی چند مرحله ای هستند، آخرین مولفه های فرآیند همبسته سازی ، مولفه تحلیل اثر[۵] و مولفه اولویت بندی[۶] هستند.

۳-۱-۱ نرمال سازی

از آنجا که هشدارهای تشخیص نفوذ از سیستم های مختلف دریافت می شوند، ضروری است به ساختار استانداردی تبدیل شوند که برای مولفه های فرآیند همبسته سازی قابل درک باشند. برای این کار، بایستی ساختار[۷] و معنای[۸] هشدار تشخیص داده می شود. این اطلاعات در پایگاه هست شناسی حسگرها نگهداری می شود. برای این کار، می توان از استاندارد پیشنهادی IDMEF [۹] استفاده نمود. البته این استاندارد، بیشتر به محدودیت های ساختاری پرداخته است و کمبود یک مدل حملات با یک شمای نامگذاری[۹] و معنای واحد، احساس می شود.

۳-۱-۲ پیش پردازش هشدارها

پس از نرمال سازی، هشدارها نام و ساختار استانداردی دارند که توسط سیستم همبسته سازی شناخته می شود. اما پیش پردازش های دیگری مورد نیاز است زیرا بعضی سیستم ها، عناصری را حذف می کنند که برای سایر مولفه های همبسته سازی ضروری هستند.

---

[1] Fusion

[2] Verification

[3] Thread Reconstruction

[4] Session Reconstruction

[5] Impact Analysis

[6] Prioritization

[7] Syntax

[8] Semantics

[9] Naming Scheme