
بسم الله الرحمن الرحیم

دانشگاه الزهرا
دانشکده فنی و مهندسی

پایان‌نامه

جهت اخذ درجه کارشناسی ارشد

رشته هوش مصنوعی

عنوان

تشخیص نفوذ روی میزبان با استفاده از راهکار سیستم‌های ایمنی مصنوعی

استاد راهنما

دکتر رضا عزمی

دانشجو

طاهره پورحبیبی

اسفند ماه سال ۱۳۸۹

کلیه دستاوردهای این تحقیق متعلق به

دانشگاه الزهرا(س) است.

تشکر و قدردانی

در اینجا برخود لازم می‌دانم که از مرکز تحقیقات مخابرات ایران به واسطه حمایت‌هایی که از این پروژه انجام داده‌اند تقدیر و تشکر نمایم.

این پایان نامه تحت قرارداد شماره ۸۹۷۱/۵۰۰ مصوب در مورخه ۸۹/۳/۲۳ تحت حمایت مرکز مخابرات ایران قرار گرفته است.

طاهره پورحبیبی

اسفند ماه ۱۳۸۹

چکیده

امروزه به دلیل اهمیت محافظت سیستم‌های اطلاعاتی از مهاجمان، سیستم‌های تشخیص نفوذ به مولفه‌های ضروری زیربنای امنیت تبدیل شده‌اند. این پژوهش نیز به تشریح یکی از راهکارهای هوش محاسباتی، سیستم‌های ایمنی مصنوعی، در تشخیص نفوذ می‌پردازد. پس از بررسی تعاریف مقدماتی و مفاهیم پایه مطرح در تشخیص نفوذ و سیستم‌های ایمنی مصنوعی دریافتیم که الگوریتم‌های انتخاب غیرخودی از جمله مهمترین شاخه‌های موجود در این سیستم‌ها در مباحث تشخیص نفوذ به شمار می‌روند و ما نیز مطالعات خود را روی این حوزه متمرکز نموده و برآن شدیم تا راهکارهایی را برای تولید هرچه بهتر تشخیص‌دهنده‌ها یعنی مجموعه تشخیص‌دهنده‌هایی با تعداد کم و میزان پوشش هرچه بیشتر و بهتر فضای غیرخودی، در الگوریتم‌های انتخاب غیرخودی ارائه دهیم؛ راهکارهایی که در فضاهای با ابعاد بالا و پایین از قابلیت‌های تشخیص خوبی برخوردار باشند. بدین ترتیب در این پژوهش دو راهکار برای تولید تشخیص-دهنده‌ها در الگوریتم‌های انتخاب غیرخودی ارائه نمودیم. الگوریتم اول مبتنی بر بکارگیری شبکه‌های عصبی RCE است و الگوریتم دوم از مفاهیم دست‌یابی به حداکثرگونه‌گونی و الگوریتم‌های جستجوی پراکندگی استفاده می‌کند تا تشخیص‌دهنده‌هایی با حداکثر میزان تشخیص و حداکثر میزان پوشش فضای غیرخودی را تولید کند.

هم‌چنین درصدد برآمدیم تا الگوریتمی برای کاهش میزان هم‌پوشانی تشخیص‌دهنده‌های تولید شده در مدل مبتنی بر RCE ارائه دهیم و به این ترتیب با صرف‌نظر از کاهش بخشی از دقت تشخیص توانستیم میزان قابل توجهی از هم‌پوشانی تشخیص‌دهنده‌ها را کاهش دهیم. نهایتا ما تنها به تشخیص خودی/غیرخودی نمونه‌های ورودی اکتفا نکرده و با ترکیب ایده‌های الگوریتم‌های انتخاب نسل در الگوریتم-های ژنتیک، مدلی برای دسته‌بندی نمونه‌های غیرخودی به یکی از چهار کلاس اصلی موجود در حملات ارائه نمودیم.

کلید واژه: تشخیص نفوذ، هوش محاسباتی، سیستم‌های ایمنی مصنوعی، شبکه عصبی RCE، انتخاب غیرخودی، انتخاب نسل، دسته‌بندی، انتخاب ویژگی.

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها ..... د

فهرست شکل‌ها ..... و

فصل ۱- مقدمه و هدف تحقیق ۱

۱-۱- مقدمه ۱

۱-۲- نفوذ و انواع آن ۱

۱-۳- تشخیص نفوذ ۳

۱-۴- فناوری‌های تشخیص نفوذ، ضعف ها و قوت ها ۶

۱-۵- ویژگی های سیستم های تشخیص نفوذ ۱۱

۱-۶- ارزیابی کارایی سیستم‌های تشخیص نفوذ ۱۳

۱-۷- هدف تحقیق ۱۶

فصل ۲- سیستم های ایمنی مصنوعی**(AIS)** و تشخیص نفوذ ۱۹

۲-۱- مقدمه‌ای بر سیستم‌های ایمنی انسانی(HIS) ۱۹

۲-۱-۱- مکانیزم انتخاب غیرخودی ۲۱

۲-۱-۲- مکانیزم انتخاب نسل ۲۲

۲-۲- سیستم ایمنی مصنوعی(AIS) ۲۶

۲-۳- سیستم های تشخیص نفوذ و سیستم های ایمنی مصنوعی(AIS) ۲۸

۲-۳-۱- ویژگی‌های سیستم های ایمنی مصنوعی برای سیستم های تشخیص نفوذ ۲۹

۲-۳-۲- شمای نمایش و معیار پیوستگی ۳۱

۲-۳-۳- مروری بر مدل‌های ایمنی مصنوعی بکارگرفته شده در تشخیص نفوذ ۳۳

۲-۳-۴- انواع الگوریتم‌های NS ۴۱
۲-۳-۵- تولید تشخیص‌دهنده‌ها ۵۳
۲-۴- مروری بر پژوهش‌های مرتبط ۵۵
فصل ۳- راهکارهای پیشنهادی ۵۸
۳-۱- الگوریتم‌های پیشنهادی ۵۸
۳-۱-۱- تشخیص خودی/غیرخودی ۵۸
۳-۱-۲- تولید تشخیص‌دهنده‌ها در راهکار مبتنی بر RCE ۵۹
۳-۱-۳- شبکه‌های عصبی RCE ۵۹
۳-۱-۴- مدل آموزش تدریجی شبکه‌های عصبی RCE ۶۱
۳-۱-۵- تولید تشخیص دهنده‌ها در راهکار مبتنی بر RCE ۶۳
۳-۱-۵-۱- توزیع تشخیص‌دهنده‌ها در راهکار مبتنی بر RCE ۶۴
۳-۲ تولید تشخیص دهنده ها در راهکار مبتنی بر جستجوی پراکندگی ۶۸
۳-۲-۱- مسئله دست یابی به حداکثر گونه گونی ۶۸
۳-۳ جستجوی پراکندگی ۶۹
۳-۳-۱- راهکار تولید پراکندگی ۷۰
۳-۳-۲- راهکار بهینه سازی ۷۱
۳-۳-۳- پیکربندی مجموعه مرجع ۷۱
۳-۳-۴- راهکار تولید زیر مجموعه ۷۲
۳-۳-۵- راهکار ترکیب ۷۲
۳-۴- طبقه‌بندی نمونه‌های غیرخودی ۷۴
۳-۵- شرح مجموعه داده ۷۶
۳-۵-۱- مجموعه داده NSL-KDD99 ..... ۷۶
۳-۵-۱-۱- استخراج ویژگی ها و نرمال‌سازی مجموعه داده ۷۷
۳-۵-۲- مجموعه لاگ فایل‌ها مربوط به نشست‌های کاربران وب ۷۸

۳-۵-۲-۱- استخراج ویژگی‌ها و نرمال‌سازی مجموعه داده ۷۹
۳-۵-۲-۲- انتخاب ویژگی‌ها ۷۹
فصل ۴- شرح نتایج ۸۲
۴-۱- نتایج شبیه سازی ۸۲
۴-۱-۱- انتخاب ویژگی ۸۲
۴-۱-۲- تشخیص خودی/غیرخودی در مدل مبتنی بر RCE ۸۴
۴-۱-۳- توزیع تشخیص دهنده ها در مدل مبتنی بر RCE ۸۸
۴-۱-۴- تشخیص خودی/غیرخودی در مدل مبتنی بر جستجوی پراکندگی ۹۰
۴-۱-۵- الگوریتم دسته‌بندی ترکیبی مبتنی بر ژنتیک و انتخاب نسل ۹۲
فصل ۵- نتیجه‌گیری، ضعف‌ها و قوت‌ها و راهکارهای آینده ۹۵
۵-۱- راهکارهای آینده ۹۹
فهرست مراجع ۱۰۱

فهرست جدول‌ها

عنوان **صفحه**

جدول ۱-۱: مزایا و معایب HIDS و NIDS ۱۰

جدول ۱-۲:ماتریس حالات تشخیص ۱۶

جدول ۲-۱: مطالعات انجام شده در زمینه الگوریتم‌هایNS با شعاع متغییر ۵۷

جدول ۴-۱: مجموعه ویژگی‌ها در NSL-KDD99 ..... ۷۷

جدول ۴-۲: کلاس‌های اصلی حملات در NSL-KDD99 ..... ۷۷

جدول ۴-۱ :نتایج حاصل از اجرای الگوریتم انتخاب ویژگی ۸۳

جدول ۴-۲ :نتایج حاصل از اجرای الگوریتم روی ۱۰ مجموعه تصادفی انتخاب شده از مجموعه داده NSL-KDD99 ..... ۸۴

جدول ۴-۳: مقایسه نتایج حاصل از انواع الگوریتم‌های v-vector روی مجموعه داده‌های KDD ۸۵

جدول ۴-۴ : بررسی رفتار v-vector در فضاهای با ابعاد مختلف ۸۶

جدول ۴-۵ :نتایج حاصل از اجرای الگوریتم روی ۳ مجموعه تصادفی انتخاب شده از مجموعه داده نشست‌ها ۸۷

جدول ۴-۶ : نتایج حاصل از اجرای الگوریتم توزیع روی ۱۰ مجموعه تصادفی انتخاب شده از مجموعه داده NSL-KDD99($k=d=10, l_{c=5}$) ۸۸

جدول ۴-۷ : نتایج حاصل از اجرای v-vector ۹۰

جدول ۴-۸: نتایج حاصل از اجرای جستجوی پراکندگی ۹۱

جدول ۴-۹: نتایج حاصل از دسته بندی حملات با استفاده از الگوریتم دسته‌بندی ترکیبی مبتنی بر ژنتیک و انتخاب نسل ۹۳

جدول ۴-۱۰: نتایج حاصل از دسته بندی داده‌های NSL-KDD99 با ۹ ویژگی با استفاده از الگوریتم‌های ژنتیک ۹۴

فهرست شکل‌ها

عنوان **صفحه**

شکل ۱-۱ : ساختار یک کلی یک سیستم تشخیص نفوذ ۵

شکل ۲-۱: توسعه B-Cell و T-Cell ۲۰

شکل ۲-۲ : اصول انتخاب نسل ۲۳

شکل ۲-۳: مراحل الگوریتم انتخاب نسل ۲۵

شکل ۲-۴ : عناصر اصلی در سیستم های ایمنی مصنوعی ۲۷

شکل ۲-۵ :چرخه عمر تشخیص دهنده ۳۴

شکل ۲-۶: مدل AIS مبتنی بر پردازش تکاملی ۳۵

شکل ۲-۷: مدل AIS چند سطحی ۳۷

شکل ۲-۸: مدل های سیستم های ایمنی مصنوعی ۳۹

شکل ۲-۹ :مدل انتخاب غیرخودی ۳۹

شکل ۲-۱۰ :مدل تشخیص خودی- غیرخودی.(الف) تولید تشخیص‌دهنده.(ب) مرحله تشخیص ۴۰

شکل ۲-۱۱ :مفهوم v-vector. (الف) تشخیص‌دهنده‌های سایز متغیر.(ب) تشخیص‌دهنده‌های سایز ثابت ۴۱

شکل ۲-۱۲ : نمایش یک مرحله تکرار الگوریتم های انتخاب غیر خودی با مقادیر حقیقی ۴۵

شکل ۲-۱۳: شبه کد مرحله تولید تشخیص دهنده ها در الگوریتم v-vector ۴۶

شکل ۲-۱۴ :تفسیرهای ممکن از یک نمونه خودی. (الف) تفسیر سنتی. (ب) تفسیر سلطه‌جوبانه ۴۷

شکل ۲-۱۵: تفسیرهای مختلف از یک مجموعه از نمونه های خودی.(الف)آستانه بزرگ.(ب) آستانه کوچک. ۴۹

شکل ۲-۱۶:وضعیت مرزی ۴۹

شکل ۲-۱۷:تشخیص دهنده ها در نواحی خودی.(الف)تفسیر سنتی.(ب) تفسیر سلطه‌جویانه.(ج) Bounady aware ۴۹

شکل ۲-۱۸: نمایش ساخت یافته از یک کوروموزوم با n مجموعه ژن متفاوت..... ۵۰

شکل ۲-۱۹: نمایش درختی کوروموزوم ۵۱

شکل ۲-۲۰: تولید تشخیص‌دهنده‌ها به کمک الگوریتم های تکاملی ۵۴

شکل ۲-۲۱: تولید و آموزش تشخیص‌دهنده‌ها ۵۵

شکل ۳-۱: ساختار یک شبکه عصبی RCE ۶۱

شکل ۳-۲: شبه کد الگوریتم تولید تشخیص‌دهنده‌ها مبتنی بر RCE ۶۴

شکل ۳-۳: میزان همپوشانی دو تشخیص دهنده، با مفهوم فاصله آن دو نمایش داده می‌شود ۶۵

شکل ۳-۴: شبه کد یک تکرار از مرحله توزیع تشخیص دهنده ۶۷

شکل ۳-۵: ساختار الگوریتم های جستجوی پراکندگی ۷۰

شکل ۴-۱: شبه کد الگوریتم Genetic Annealing..... ۸۱

شکل ۴-۱:(الف)مقایسه میزان هم پوشانی تشخیص دهنده ها قبل و بعد از توزیع ، (ب) مقایسه دقت تشخیص دهنده ها در تشخیص حملات قبل و بعد از توزیع ۸۹

شکل ۴-۲: (الف)مقایسه fn قبل و بعد از توزیع، (ب) مقایسه fa قبل و بعد از توزیع ۸۹

شکل ۴-۳: مقایسه نتایج حاصل از دسته بندی حملات با استفاده از الگوریتم دسته‌بندی ترکیبی مبتنی بر ژنتیک و انتخاب نسل ۹۳

شکل ۴-۴: مقایسه نتایج حاصل از دسته‌بندی داده های NSL-KDD99 با ۹ ویژگی در الگوریتم ژنتیک و مدل دسته‌بندی ارائه شده ۹۴

شکل ۵-۱: ساختار سیستم تشخیص نفوذ ارائه شده مبتنی بر مدل های مورد بحث ۹۹

فصل ۱– مقدمه و هدف تحقیق

۱–۱– مقدمه

با توجه به کاهش هزینه‌های دسترسی به اینترنت و پردازش اطلاعات، آسیب‌پذیری سازمان‌ها نسبت به تهدیدات بالقوه مانند مهاجمان شبکه نیز رو به افزایش است. این مساله، نیاز به یک تراکنش ایمن و بی-خطر را به واسطه استفاده از فایروال‌ها، سیستم‌های تشخیص نفوذ، پنهان‌سازی[۱]، اعتبار سنجی[۲] و دیگر چاره-سازی‌های نرم‌افزاری و سخت‌افزاری، نمایان می‌سازد. گونه‌های زیادی از سیستم‌های تشخیص نفوذ وجود دارند که امکان تشخیص حملات را با کمک امضاءهایی که از قبل تعریف شده‌اند، برای مسئولین و مهندسین امنیت فراهم می‌کنند. در بسیاری از سیستم‌ها، به‌جهت پیچیدگی‌های سیستمی، پیکربندی و استفاده غیر-متعارف کاربران قانونی، امکان ممانعت کامل از حملات وجود ندارد. به‌همین جهت، تشخیص نفوذ به یکی از جنبه‌های اساسی تلاش‌های سال‌های اخیر امنیت کامپیوتر تبدیل شده است.

۱–۲– نفوذ و انواع آن

نفوذ، به مجموعه فعالیت‌هایی گفته می‌شود که تلاش می‌کنند مکانیزم‌های امنیتی سیستم‌های کامپیوتری را پشت سر بگذارند[۱]. بنابراین، شامل مجموعه فعالیت‌هایی هستند که ویژگی‌هایی از قبیل درستی[۳]، قابلیت دسترسی و محرمانگی منابع سیستم و شبکه را تهدید می‌کنند[۱][۲].

نمونه‌هایی از تهدیدها عبارت‌اند از:

- عدم پذیرش سرویس‌ها (DOS)[۱]

---

[1]-Encryption

[2]-Authentication

[3]-Integrity

تهدیدی است که طی آن، مهاجم منابع حافظه و منابع محاسباتی را بسیار مشغول می‌کند، به‌طوری که دیگر قادر به اجرای درخواست‌های قانونی نخواهند بود و یا این‌که دسترسی کاربران قانونی به یک ماشین را نمی‌پذیرند[۱][۳][۴].

گونه‌های مختلفی از این تهدید وجود دارد که مهمترین آن‌ها سرریز شدن بافر[۲] است که زمانی رخ می‌دهد که یک برنامه بدون آن‌که مطمئن باشد که داده‌ها معتبر باقی می‌مانند، داده‌های زیادی را به درون یک بافر ایستا[۳] کپی می‌کند[۱][۳][۴].

- حمله کاربر به ریشه(U2R)[۴]

تهدیدی است که در آن، مهاجم با دست‌یابی به دسترسی‌های یک کاربر نرمال روی یک سیستم، نفوذ خود را آغاز می‌کند و قادر به انجام فعالیت‌های آسیب‌پذیر برای دسترسی ریشه‌ای به سیستم خواهد بود.

- اسکن[۵]

نوعی بازدید مقدماتی روی یک شبکه یا یک میزبان ویژه است. هدف از اسکن کردن پورت‌ها، مشخص نمودن آن دسته از پورت‌هایی است که باز هستند و در نتیجه آن، مشخص کردن سرویس‌هایی است که روی یک سیستم در حال اجرا هستند. این نتایج می توانند در یک استفاده صحیح و به‌عنوان بخشی از بازبینی‌های مربوط به امنیت، توسط مدیر سیستم مورد استفاده قرارگیرند و نیز در یک استفاده ناصحیح، توسط مهاجمانی که به دنبال انجام عملیات روی سرویس‌های درحال اجرا روی پورت‌های باز کامپیوتر هستند، مورد استفاده قرارگیرند[۱][۳].

- حمله به کاربر از راه دور(R2L)[۶]

---

[1]-Denial Of Service

[2] -Buffer Over Flow

[3]-Static Buffer

[4] - User to root attack(U2R)

[5] -Scan

[6] - Remote to User attacks(R2L)

حمله‌ای است که طی آن یک کاربر، بسته‌هایی را از طریق اینترنت برای یک ماشین ارسال می‌کند و کاربر از دسترسی لازم برای نمایش آسیب‌پذیری‌های ماشین و بهره‌برداری از مزایایی که یک کاربر محلی روی آن کامپیوتر دارد، برخوردار نیست[۴].

- تفحص[1]

حمله‌ای است که طی آن، هکر، یک کامپیوتر یا یک وسیله شبکه‌بندی را به‌منظور مشخص‌کردن نقاط ضعف یا نقایصی که بعدها می‌تواند برای به‌خطر انداختن سیستم مورد استفاده قرار بگیرد، بررسی می‌کند[۴].

۱-۳-تشخیص نفوذ

تشخیص نفوذ، فرآیند مونیتورینگ اتفاقات در حال رخداد در یک سیستم کامپیوتری یا شبکه و آنالیز آن‌ها به‌منظور مشخص نمودن تهدیدهایی مانند نفوذ و استفاده بدون اجازه فایل‌ها و یا تغییر آن‌ها می‌باشد[۱][۵][۶]. این فرایند در سه مرحله انجام می‌شود که عبارت‌انداز[۱]:

- مونیتورینگ و آنالیز ترافیک
- مشخص نمودن فعالیت‌های غیر نرمال
- ارزیابی شدت فعالیت‌های غیرنرمال و اعلام هشدارهای مناسب

هدف اصلی سیستم‌های تشخیص نفوذ، تشخیص استفاده غیرمجاز و یا سوء استفاده از سیستم‌های کامپیوتری، چه توسط کارمندان داخلی و چه توسط مهاجمان خارجی است[۱]. به عبارت دیگر یک سیستم تشخیص نفوذ فعالیت‌های رخ داده در یک سیستم و یک محیط مشخص را مونیتور می‌کند و تصمیم می‌گیرد که آیا این فعالیت‌ها نشانه وقوع یک حمله هستند و یا این‌که معرف استفاده قانونی از محیط هستند[۷].

سیستم‌های تشخیص نفوذ از چهار مولفه اصلی به شرح زیر تشکیل شده‌اند[۱][۸]:

---

[1]-Probing

- سنسورها و کاوشگرها، که تولید کننده فعالیت‌های امنیتی هستند. آن‌ها ترافیک شبکه را پیگیری می‌کنند، رفتارهای سیستم و فایل‌ها را ثبت و داده‌ها را به رویدادهای قابل استفاده توسط مونیتورهای IDS منتقل می‌کنند.

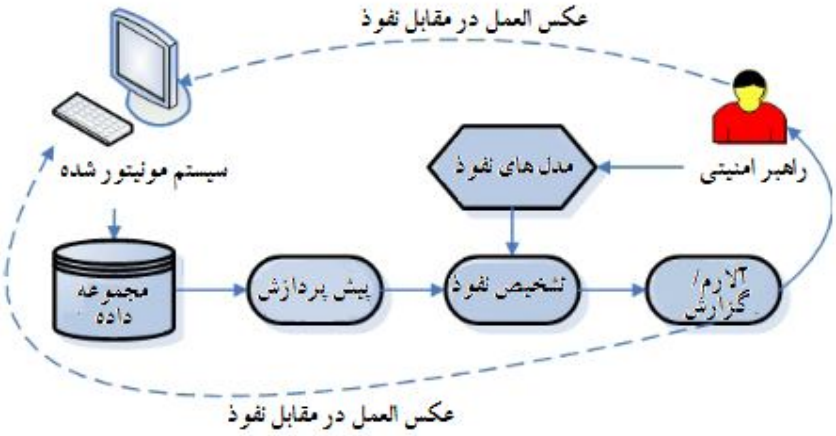
- کنسول‌ها و مونیتورها، برای مونیتورینگ فعالیت‌ها و اعلام هشدارها و کنترل سنسورها مورد استفاده قرار می‌گیرند. در واقع مونیتور مهمترین بخش یک IDS محسوب می‌گردد که رویدادها را از سنسورها دریافت می‌کند؛ سپس این رویدادها برعلیه مدل‌های رفتاری IDS و به‌طور بالقوه برای تولید مدل‌های بروزسانی و هشدارهایی به‌کار می‌روند که بیان‌گر رخدادهای قابل توجه در امنیت یک سیستم‌اند و ممکن است به سمت مونیتورهای سطح بالاتر و یا واحدهای برطرف کننده[1] فرستاده شوند.

- موتور مرکزی یا برطرف کننده، فعالیت‌های ثبت شده توسط سنسورها را در یک پایگاه اطلاعاتی ثبت می‌کنند و عکس العمل مناسب مانند ثبت وقایع، تغییر رفتار مولفه‌های سطح پایین‌تر، پیکربندی مجدد دیگر مکانیزم‌های امنیتی مانند افزودن فایروال و یا آگاه‌سازی اپراتور را تعیین می‌کنند.

- کنترلرها، به جهت قابلیت سهولت پیکربندی، در IDS های توزیع شده بسیار مورد استفاده قرار می‌گیرند. کنترلرها نقطه مجردی از مدیریت و بازبینی در یک IDS را فراهم کرده و در یک جایگاه نظارتی، موجب از سرگیری فعالیت مولفه‌هایی که دچار شکست شده‌اند، می‌گردند.

(شکل۱-۱) ساختار یک سیستم تشخیص نفوذ را نشان می‌دهد. خطوط به‌هم پیوسته نشان‌دهنده جریان داده/کنترل است، درحالی‌که خطوط نقطه‌چین، نشان‌دهنده عکس العمل به تهدیدات هستند[۹].

[1]-resolver



شکل ۱-۱ : ساختار یک کلی یک سیستم تشخیص نفوذ

چهار مرحله اصلی از فرآیند تحلیل در همه انواع سیستم‌های تشخیص نفوذ وجوددارند. این چهار مرحله عبارت‌انداز پیش پردازش، آنالیز، عکس‌العمل و پالایش.

پیش پردازش، شامل فرآیندهای طبقه‌بندی مختلفی به‌منظور قالب‌بندی اطلاعات گردآوری شده از سیستم تشخیص نفوذ است. مرحله آنالیز شامل مقایسه بین پایگاه دانش و داده‌های طبقه‌بندی شده است. داده‌های موجود در این مرحله می‌توانند به‌صورت یک تهدید ثبت شوند. عکس‌العمل می‌تواند به‌صورت دستی بعد از آنالیز و یا به‌صورت اتوماتیک حین حملات جاری انجام شود که شامل فعالیت‌هایی چون اعلام هشدار از طریق پیام کوتاه، ایمیل و تله SNMP و... است. نهایتاً، در مرحله پالایش، تلاش می‌شود که تدابیر امنیتی اعمال شده در سیستم تشخیص نفوذ مجدداً تنظیم گردند تا به این ترتیب شانس وقوع تعداد مثبت‌های کاذب[1] (fp) در سیستم کاهش یابد[۴].

[1] - false positive

۱-۴-فناوری‌های تشخیص نفوذ، ضعف ها و قوت ها

سیستم‌های تشخیص نفوذ، نرم افزارهایی برای تشخیص و ممانعت از استفاده غیرمجاز از کامپیوترها و سیستم‌های شبکه هستند که روش‌های زیادی برای طبقه بندی آن‌ها وجود دارد: راهکارهای تحلیلی و تقسیم بندی بر اساس محل قرارگیری سیستم‌های تشخیص نفوذ.

راهکارهای تحلیلی شامل دو دسته اند: تشخیص سوءاستفاده یا تشخیص مبتنی بر امضاء[1] (تشخیص مبتنی بر پایگاه دانش[۷]) و تشخیص ناهنجاری[2](تشخیص مبتنی بر رفتار[۷]) . راهکارهای تشخیص مبتنی بر امضاء، به‌منظور تشخیص استفاده‌های غیر مجازی که قبلا شناخته شده‌اند و با استفاده از روش‌های تطبیق الگو، شبکه و سیستم را بررسی می‌کنند[۹][۱۰].

درمقابل، راهکارهای تشخیص ناهنجاری، بر مبنای پروفایلی از رفتارهای نرمال سیستم یا شبکه تصمیم‌گیری می‌کنند و اغلب براساس روش‌های آماری و تکنیک‌های یادگیری ماشین عمل می‌کنند. هر فعالیتی که با این پروفایل تطبیق نداشته باشد، غیرمتعارف تصور می‌گردد[۹][۱۰]. در هر یک از این روش‌ها، ضعف‌ها و قوت‌هایی وجود دارد. تشخیص مبتنی بر امضاء، اغلب دارای نرخ مثبت کاذب(fp)[3] خیلی پایینی است که نشان‌دهنده نرخ خطا در مواردی است که نفوذ تشخیص داده نشده‌اند[۹][۱۱]. به‌همین دلیل، این راهکارها بیشتر در سیستم‌های تجاری مورد استفاده قرارمی‌گیرند که در هرصورت، قادر به تشخیص حملات جدید و مبهم نخواهند بود و همین امر موجب بالا بودن نرخ منفی کاذب[4](fn) آن‌ها می‌گردد که نمایش دهنده نرخ خطا در مواردی است که در تشخیص، خطا رخ داده است[۱۲][۵]. یک راه برای حل این مشکل، بروزرسانی منظم پایگاه‌داده است؛ این‌کار می تواند به‌صورت دستی انجام شود که دشوار و مستلزم صرف هزینه‌های زمانی بسیار زیاد است و یا اینکه به‌صورت خودکار و بااستفاده از الگوریتم‌های یادگیری نظارت

[1]- misuse detection

[2]-anomaly detection

[3] -false positive

[4] - false negative

شده[1](SL) انجام شود که متاسفانه بازیابی چنین مجموعه داده‌ای به‌جهت اینکه نیازمند برچسب‌گذاری هر یک از نمونه‌ها به‌صورت نمونه‌های نرمال و غیر نرمال است، بسیار پر هزینه است. راهکار دیگری که برای حل این مشکل وجود دارد، استفاده از راهکار تشخیص نفوذ مبتنی بر ناهنجاری است که توسط دنینگ[2] ارائه شده است[۹]. راهکارهای مبتنی بر ناهنجاری، رفتارهای غیرمعمول مانند ناهنجاری، مصرف بسیار بالا و بیش از حد معمول پردازنده[3]، ترافیک بالای شبکه و تعداد فایل‌های ارسال شده برای یک کاربر در طول یک بازه زمانی مشخص را بررسی می‌کنند[۵]. راهکارهای تشخیص ناهنجاری دو دسته اند[۹][۱۳]. تشخیص ناهنجاری ایستا[4]، در تشخیص دهنده‌های ناهنجاری فرض می‌شود که بخشی از سیستمی که در حال مونیتور شدن است بدون تغییر باقی می‌ماند. تشخیص دهنده‌های ناهنجاری معمولا تنها بخش نرم‌افزاری یک سیستم را مورد توجه قرار می‌دهند و بر این فرض مبتنی هستند که بخش‌های سخت‌افزاری نیازی به چک شدن ندارند. بخش ایستای یک سیستم شامل کدهای سیستم و داده‌های ثابت سیستم است که عملکرد صحیح سیستم وابسته به آنهاست. بخش‌های ایستای سیستم را می‌توان به فرمت رشته‌ای باینری و یا مجموعه‌ای از رشته‌ها مانند یک فایل نشان داد؛ چنانچه بخش ایستای سیستم در هر صورتی از فرم اصلی خود منحرف شود، نشان‌دهنده وقوع خطا بوده و یا اینکه یک مهاجم وارد بخش ایستای سیستم شده است[۱۳]. تشخیص ناهنجاری پویا[5]، در این روش، الگوهایی از عادات رفتاری کاربران و یا تاریخچه ای از کاربران شبکه/ میزبان‌ها را جمع‌آوری می‌کنند؛ این الگوها اغلب پروفایل نامیده می‌شوند[۹].

تشخیص دهنده‌های ناهنجاری، قادر به تشخیص حملات جدید هستند اما همچنانfp بسیار زیادی تولید می‌کنند و این بدان معناست که پروفایل مربوط به رفتارهای نرمال همیشه باید پویا و به‌روز باشد[۱۲].

---

[1]-Supervised Learning (SL)

[2]-Denning

[3] - cpu

[4]-Static Anomaly Detection

[5]-Dynamic Anomaly Detection

نرخ fp و fn تولید شده در راهکارهای تشخیص ناهنجاری نسبت به راهکارهای تشخیص مبتنی بر امضاء بسیار زیاد است[۵].

مشکل اصلی که در راهکارهای تشخیص مبتنی بر ناهنجاری وجود دارد، مشکل تشخیص مرز بین رفتارهای نرمال و غیرنرمال است که ناشی از نقص و ناکارآمدی داده‌ها در مرحله آموزش هستند. مشکل دیگری که به ویژه در تشخیص ناهنجاری پویا مطرح است، سازگارشدن با تغییرات دائمی رفتارهای نرمال است.

راهکارهای مدل‌سازی تشخیص ناهنجاری شامل مدل‌های آماری، راهکارهای مدل‌سازی مبتنی بر سیستم‌های ایمنی، راهکارهای بازبینی پروتکل، راهکارهای بازرسی فایل، راهکارهای بررسی عیب، راهکارهای مبتنی بر شبکه‌های عصبی و راهکارهای لیست سفید[۱] بوده و از جمله راهکارهای مدل‌سازی تشخیص امضاء نیز می‌توان به مدل تطبیق ظاهری، مدل آنالیز انتقال حالت، زبان‌های اختصاصی، الگوریتم‌های ژنتیک و هشدارهای تهدید[۲] اشاره نمود(برای مطالعه بیشتر به[۸][۱۴] مراجعه کنید).

دسته‌بندی دیگری که وجود دارد، بر اساس محل قرارگیری سیستم‌های تشخیص نفوذ است که از این جنبه، سیستم‌های تشخیص نفوذ دو دسته اند: سیستم‌های مبتنی بر شبکه[۳] و سیستم‌های مبتنی بر میزبان[۴]. سیستم‌های مبتنی بر میزبان مثل tripware در[۱۵]، روی هر میزبانی[۵] که نیازمند مونیتورینگ است، وجود دارند و داده‌های مرتبط با این میزبان را جمع‌آوری می کنند و معمولا فایل‌ها، ترافیک شبکه به سمت یک میزبان و یا از سوی یک میزبان و نیز اطلاعات مربوط به فرآیندهای در حال اجرا روی یک میزبان را ثبت می‌کنند. در مقابل، سیستم‌های مبتنی بر شبکه هستند که روی یک ماشین جداگانه به‌نام سنسور و در شبکه‌ای شامل میزبان‌هایی که باید مونیتور شوند، اجرا می‌گردند.

---

[1] - white listing

[2] - Burglar alarm

[3]-Network based

[4] -Host Based

[5]-Host