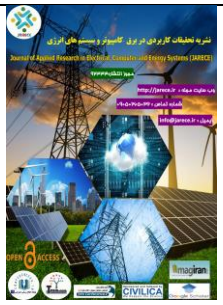
Vol. 2, No. 6, Jul-Sep 2024, (1-20)

Journal of Applied Research in Electrical, Computer and Energy Systems (JARECE)

نشریه تحقیقات کاربردی در برق ، کامپیوتر و سیستم های انرژی

دوره ۲، شماره ۶، تابستان ۱۴۰۳ (۲۰-۱)

journal homepage: https://jarece.ir/



مروری جامع بر تکنیکهای سیستم تشخیص نفوذ

امین داستانپور

بخش مهندسی کامپیوتر موسسه آموزش عالی کرمان (amindastanpoure@gmail.com)

چکیده

شبکه داده یا شبکه کامپیوتری شبکه ای از مخابرات است که در آن از رایانه ها برای تبادل داده استفاده می شود. شکل تبدیل داده ها بسته نامیده می شود، رسانه های بی سیم یا رسانه های کابلی برای ایجاد پیوندها در شبکه (اتصالات) بین گره ها استفاده می شوند. اینترنت به عنوان شناخته شده ترین شبکه کامپیوتری شناخته می شود. در شبکه های کامپیوتری ، حمله به عنوان هرگونه تلاش برای تخریب، افشای، تغییر، غیرفعال کردن، سرقت، دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی تعریف می شود. طبقه بندی مهاجمان را نشان می دهدکه به دو دسته محاجم خارجی وداخلی تقسیم میشوند. مهاجم خارجی یک حمله خارجی است، که فردی از خارج از شبکه سعی می کند آن را دور بزند یا به سیستم های ایمن نفوذ کند. طرح کلی مهاجم خارجی به منظور جلوگیری از حملات این نوع مهاجمان، دانشمندان استفاده از فایروال را پیشنهاد می کنند. امنیتی شبکه تعریف می شود که ترافیک شبکه ورودی و خروجی را بر اساس مجموعه قوانین اعمال شده کنترل می کند. فایروال مانعی بین یک شبکه داخلی قابل اعتماد و امن و شبکه های دیگر (مثلاً اینترنت) قرار می دهد که فرض می شود ایمن و قابل اعتماد نیست. مشکل مهم فایروال این است که فایروال نمی تواند شبکه را از مهاجمان داخلی (خودی) محافظت کند. به عبارت دیگر، یک فایروال توانایی جلوگیری از تک تک کاربرانی که از مودم ها برای شماره گیری داخل یا خارج از شبکه استفاده می کنند و حمله از دیوار آتش دور می زند را ندارد. به منظور جلوگیری از حملات این نوع مهاجمان، مدیر از سیستم تشخیص نفوذ استفاده می کند. سیستم تشخیص نفوذ (IDS) یک دستگاه یا نرم‌افزار است که فعالیت‌های شبکه یا سیستم را برای فعالیت‌های مخرب یا نقض خط‌مشی نظارت می‌کند و گزارش‌هایی را به یک ایستگاه مدیریت می‌دهد. طرح کلی اثرات IDS در حفاظت از شبکه ها در شکل علاوه بر این، یک فایروال می تواند اتصال را مسدود کند، در حالی که یک سیستم تشخیص نفوذ (IDS) نمی تواند اتصال را مسدود کند و فقط هرگونه تلاش برای نفوذ را به مدیر امنیتی هشدار می دهد. در این مقاله به بیان اهمیت تشخیص نفوذ و بررسی انواع آن به علاوه به بررسی تکنیکهای آن میپردازد.

واژگان کلیدی: مروری, امنیت شبکه, سیستم تشخیص نفوذ,تکنیکهای امنیت شبکهتکنیکهای, سیستم تشخیص نفوذ ,IDS

مروری بر تحقیق

شبکه داده یا شبکه کامپیوتری شبکه ای از مخابرات است که در آن از رایانه ها برای تبادل داده استفاده می شود. شکل تبدیل داده ها بسته نامیده می شود، رسانه های بی سیم یا رسانه های کابلی برای ایجاد پیوندها در شبکه (اتصالات) بین گره ها استفاده می شوند. اینترنت به عنوان شناخته شده ترین شبکه کامپیوتری شناخته می شود [1].

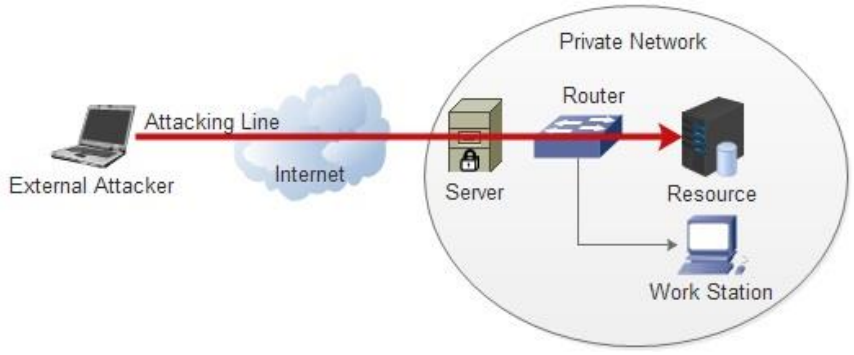
بر اساس گزارش منتشر شده توسط اداره تحقیقات فدرال (FBI) مرکز شکایات جرایم اینترنتی (IC3) 262813 شکایت مصرف‌کننده با 781841611 دلار زیان دریافت کرد که 48.8٪ افزایش در مقایسه با 5814411101 دلار از دست دادن دلار از سال 2018 تاکنون است [2]. در نتیجه این موضوع توجه را به سمت استفاده از تکنیک ایمن کارآمدتر برای ایجاد ارتباط و ارتباط ایمن تر جلب می کند.

در شبکه های کامپیوتری ، حمله به عنوان هرگونه تلاش برای تخریب، افشای، تغییر، غیرفعال کردن، سرقت، دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی تعریف می شود. به طور کلی، دو گروه از مهاجمان وجود دارد که عبارتند از مهاجم خارجی و مهاجم داخلی [3]. شکل 1.1 طبقه بندی مهاجمان را نشان می دهد.

شکل 1.1 طبقه بندی مهاجمان

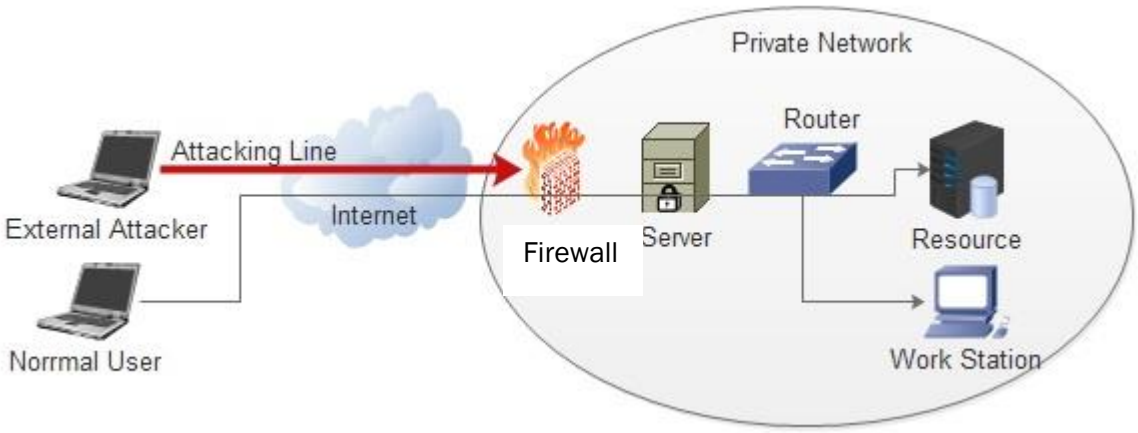
حمله خارجی

مهاجم خارجی یک حمله خارجی است، که فردی از خارج از شبکه سعی می کند آن را دور بزند یا به سیستم های ایمن نفوذ کند [4]. شکل 1.2 مفهوم ساده مهاجم خارجی را نشان می دهد.



شکل 1.2 طرح کلی مهاجم خارجی

به منظور جلوگیری از حملات این نوع مهاجمان، دانشمندان استفاده از فایروال را پیشنهاد می کنند [5]امنیتی شبکه تعریف می شود که ترافیک شبکه ورودی و خروجی را بر اساس مجموعه قوانین اعمال شده کنترل می کند. فایروال مانعی بین یک شبکه داخلی قابل اعتماد و امن و شبکه های دیگر (مثلاً اینترنت) قرار می دهد که فرض می شود ایمن و قابل اعتماد نیست. طرح کلی تکنیک فایروال در شکل 1.3 نشان داده شده است.



شکل 1.3 طرح کلی تکنیک فایروال

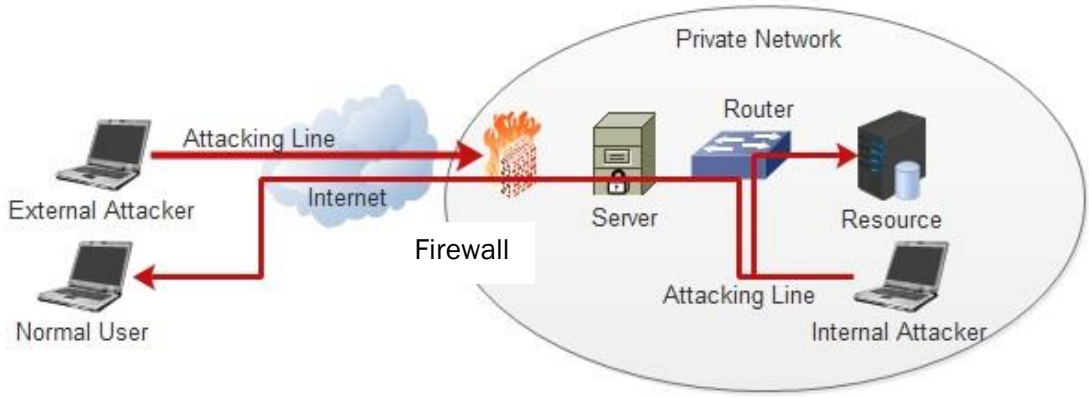
یک فایروال دسترسی به شبکه شما را با غربالگری ترافیک و تصمیم گیری اینکه کدام بسته ها باید در [6]. فایروال پورت هایی را که شبکه شما را به اینترنت متصل می کنند نظارت می کند و بسته های داده را قبل از عبور از آنها بررسی می کند. فایروال می‌تواند بسته‌ای را بپذیرد، آن را رها کند (آن را از وجود پاک کند) یا آن را رد کند و آن را به فرستنده بازگرداند [7].

حمله داخلی

در مورد حمله داخلی، شخصی (مهاجم) از داخل مانند یک کارمند ناراضی به شبکه حمله می کند. حملات داخلی می توانند مخرب یا غیر مخرب باشند. خودی‌های مخرب عمداً اطلاعات را استراق سمع، سرقت یا آسیب می‌رسانند. استفاده از اطلاعات به شیوه ای متقلبانه؛ یا دسترسی به سایر کاربران مجاز را رد کنید. حملات غیر مخرب معمولاً ناشی از بی دقتی، عدم آگاهی یا دور زدن عمدی امنیت به دلایلی برای انجام یک کار خاص است [8].

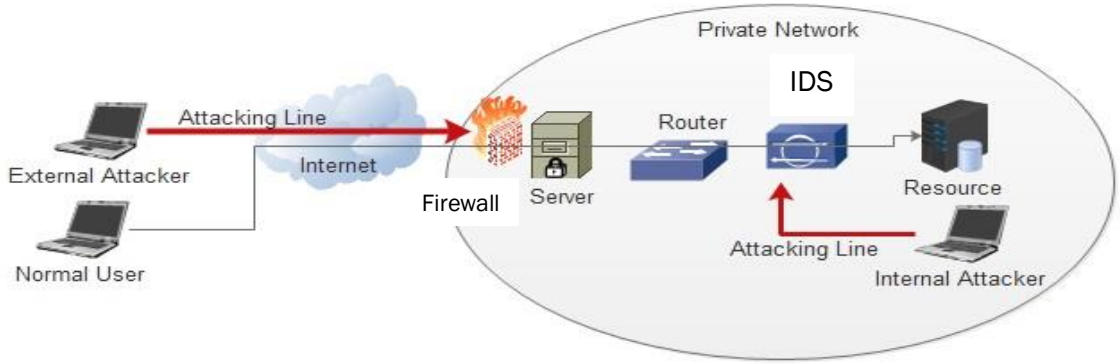
علاوه بر این، مهاجم سعی می کند با مهاجم داخلی به شبکه حمله کند. مشکل مهم فایروال این است که فایروال نمی تواند شبکه را از مهاجمان داخلی (خودی) محافظت کند. به عبارت دیگر، یک فایروال توانایی جلوگیری از تک تک کاربرانی که از مودم ها برای شماره گیری داخل یا خارج از شبکه استفاده می کنند و حمله از دیوار آتش دور می زند را ندارد [9]. بنابراین، کارکنانی که دارای رفتار نادرست یا بی احتیاطی هستند، توسط فایروال ها قابل کنترل نیستند. بر این اساس، سیاست های امنیتی که شامل گذرواژه ها و حساب های کاربری می شوند باید به شدت اجرا شوند. اینها مسائل مدیریتی هستند که باید در طول برنامه ریزی هر سیاست

امنیتی در نظر گرفته شوند. اما، این مشکلات را نمی توان تنها با فایروال حل کرد [10]. طرح اشکالات دیوار آتش در شکل 1.4 نشان داده شده است.



شکل 1.4 طرح اشکالات فایروال

به منظور جلوگیری از حملات این نوع مهاجمان، مدیر از سیستم تشخیص نفوذ استفاده می کند. سیستم تشخیص نفوذ (IDS) یک دستگاه یا نرم‌افزار است که فعالیت‌های شبکه یا سیستم را برای فعالیت‌های مخرب یا نقض خط‌مشی نظارت می‌کند و گزارش‌هایی را به یک ایستگاه مدیریت می‌دهد [11]. طرح کلی اثرات IDS در حفاظت از شبکه ها در شکل 1.5 نشان داده شده است



شکل 1.5 طرح کلی اثرات IDS در حفاظت از شبکه ها

می‌توانیم تصور کنیم که فایروال به‌عنوان پرسنل امنیتی در گیت و یک دستگاه IDS به‌عنوان دوربین امنیتی بعد از دروازه ایفای نقش می‌کند. علاوه بر این، یک فایروال می تواند اتصال را مسدود کند، در حالی که یک سیستم تشخیص نفوذ (IDS) نمی تواند اتصال را مسدود کند و فقط هرگونه تلاش برای نفوذ را به مدیر امنیتی هشدار می دهد [12].

بر اساس گزارش منتشر شده توسط شرکت Symantec (شرکت ضد ویروس) برای ماه نوامبر 2013، تعداد حملات داخلی افزایش یافته است، 5965 حمله مخرب جدید کشف شده است. با این نوع مهاجم، شرکت بزرگ می تواند 2.4 میلیون دلار خسارات مالی مستقیم و هزینه های اضافی برای آن هزینه کند. برای یک شرکت متوسط یا کوچک، یک حمله هدفمند می تواند به معنای حدود

92000 دلار خسارت باشد [13]. بنابراین، سیستم‌های تشخیص نفوذ اخیراً به دلیل نظارت بر ترافیک شبکه با شناسایی منابع سوء استفاده شده، استفاده غیرمجاز استفاده می‌شوند [14]. سیستم های تشخیص نفوذ دارای وظایف زیر هستند:

1. نظارت و تجزیه و تحلیل فعالیت های کاربر و سیستم
2. ممیزی پیکربندی ها و آسیب پذیری های سیستم
3. ارزیابی یکپارچگی سیستم های حیاتی و فایل های داده
4. تجزیه و تحلیل آماری الگوهای فعالیت بر اساس تطبیق با حملات شناخته شده
5. تجزیه و تحلیل فعالیت غیرعادی و ممیزی سیستم عامل

پس زمینه مشکل

IDS دو نوع دارد. سیستم های تشخیص نفوذ مبتنی بر شبکه (NIDS) و مبتنی بر میزبان IDS .(HIDS) دو روش برای تشخیص دارد، یعنی IDS مبتنی بر امضا و IDS مبتنی بر ناهنجاری آماری [15].

سیستم های تشخیص نفوذ شبکه

سیستم‌های تشخیص نفوذ شبکه (NIDS) در یک نقطه یا نقاط استراتژیک در شبکه قرار می‌گیرند تا ترافیک همه دستگاه‌های موجود در شبکه را نظارت کنند [16]. برای تجزیه و تحلیل ترافیک عبوری در کل زیرشبکه عمل می‌کند، در حالت بی‌وقفه کار می‌کند، و ترافیکی را که روی زیرشبکه‌ها ارسال می‌شود به کتابخانه حملات شناخته شده تطبیق می‌دهد. هنگامی که حمله شناسایی شد یا رفتار غیرعادی کشف شد، هشدار برای مدیر ارسال می شود [17]. نمونه ای از استفاده از NIDS در زیرشبکه نصب می شود، جایی که فایروال ها قرار دارند تا ببینند آیا کسی در تلاش است تا به دیوار آتش نفوذ کند یا خیر [18].

سیستم های تشخیص نفوذ میزبان

سیستم‌های تشخیص نفوذ میزبان (HIDS) در هاست‌ها یا دستگاه‌های جداگانه در شبکه اجرا می‌شوند [19]. HIDS فقط بسته های ورودی و خروجی از دستگاه را نظارت می کند و در صورت شناسایی فعالیت مشکوک به کاربر یا مدیر هشدار می دهد. یک عکس فوری از فایل‌های سیستم موجود می‌گیرد و آن را با عکس فوری قبلی [20]. اگر فایل‌های مهم سیستم اصلاح یا حذف شده باشند، هشدار برای بررسی به مدیر ارسال می‌شود. نمونه ای از استفاده از HIDS را می توان در ماشین های حیاتی ماموریت مشاهده کرد، که انتظار نمی رود تنظیمات خود را تغییر دهند [21].

IDS مبتنی بر امضا

IDS مبتنی بر امضا، بسته‌های شبکه را کنترل می‌کند و آنها را با پایگاه داده‌ای از امضاها یا ویژگی‌های تهدیدات مخرب شناخته شده مقایسه می‌کند. این روش مشابه اکثر نرم افزارهای آنتی ویروس است که بدافزارها را شناسایی می کنند. مشکل اصلی IDS

مبتنی بر امضا این است که بین کشف تهدید جدید و امضای شناسایی تهدیدی که برای IDS شما اعمال می شود، تاخیر وجود دارد. بنابراین، IDS قادر به تشخیص تهدید جدید در طول آن زمان تاخیر نخواهد بود [22].

IDS مبتنی بر ناهنجاری آماری

یک IDS مبتنی بر ناهنجاری ترافیک شبکه را رصد می کند و آن را با یک خط مبنا تعیین شده مقایسه می کند [23]. خط مبنا مشخص می کند که "چه چیزی برای آن شبکه "عادی" است؟، "چه نوع پهنای باندی معمولا استفاده می شود؟"، "چه پروتکل هایی استفاده می شود؟"، "چه پورت ها و دستگاه هایی به طور کلی به یکدیگر متصل می شوند؟"، و هشدار می دهد. مدیر یا کاربر هر زمان که ترافیک به صورت غیرعادی یا به طور قابل توجهی متفاوت از خط پایه تشخیص داده شود. اشکال اصلی IDS مبتنی بر ناهنجاری این است که اگر خطوط پایه به طور هوشمندانه پیکربندی نشده باشند، ممکن است یک هشدار مثبت کاذب برای استفاده مجاز از پهنای باند ایجاد کند [24].

استفاده از یادگیری ماشین برای IDS مبتنی بر ناهنجاری آماری

در IDS مبتنی بر ناهنجاری، هنگام شناسایی حملات، ویژگی های زیادی وجود دارد که باید در نظر گرفته شود. این سیستم باید با حجم عظیمی از ترافیک شبکه با توزیع بسیار نامتعادل داده مقابله کند. بنابراین، تشخیص رفتار عادی در مقابل رفتار غیرعادی چالش است [25]. با حجم عظیمی از ترافیک، داده های بیشتری باید در هنگام تشکیل الگوها در نظر گرفته شود. این احتمال نرخ مثبت کاذب بالا را افزایش می دهد.

هدف یادگیری ماشینی یادگیری و/یا کشف و همچنین سازگاری با شرایط در حال تغییر در طول زمان و بهبود عملکرد آن در برخی وظایف در طول زمان است. در سیستم تشخیص نفوذ، الگوریتم های یادگیری ماشین ابتدا با ورودی های شناخته شده برای "یادگیری" الگوهای حمله آموزش داده می شوند و سپس با حملات ورودی ناشناخته اعتبارسنجی می شوند. علاوه بر قابلیت الگوریتم‌های یادگیری ماشین برای تشخیص الگوهای حمله جدید، قابل توجه است که این الگوریتم‌ها می‌توانند در مورد مجموعه داده‌های عظیم با ویژگی‌های نامربوط و زائد نیز مورد استفاده قرار گیرند و تنها چند ویژگی مهم را برای بهینه‌سازی فرآیند تشخیص در نظر بگیرند. [26].

یکی از مسائل مهم یادگیری ماشین طبقه بندی است. سوالی که از این جمله مطرح می شود این است که "چگونه مجموعه ای از دسته ها (زیرجمعیت ها) را طبقه بندی کنیم؟" به عنوان مثال، هنگامی که ایمیل دریافت می‌شود، به کلاس‌های "هرزنامه" یا "غیر هرزنامه" اختصاص داده می‌شود یا تشخیصی را به یک بیمار مشخص می‌دهد که بر اساس ویژگی‌های مشاهده شده بیمار (جنسیت، فشار خون، وجود یا عدم وجود برخی موارد خاص) توضیح داده شده است. علائم). [27].

در اصطلاح یادگیری ماشینی، طبقه بندی نمونه ای از یادگیری تحت نظارت در نظر گرفته می شود. یادگیری تحت نظارت از مجموعه آموزشی مشاهدات به درستی شناسایی شده یاد می گیرد [28]. مهم‌ترین الگوریتم‌های طبقه‌بندی عبارتند از: سیستم استنتاج فازی عصبی تطبیقی (ANFIS)، شبکه عصبی فازی (FNN)، شبکه‌های عصبی مصنوعی (ANN) و ماشین بردار پشتیبان (SVM)

به منظور بهبود کارایی مدل یادگیری ماشین، تکنیک‌های بهینه‌سازی به مدل مرتبط می‌شوند. بهینه سازی انتخاب بهترین عنصر (با توجه به برخی معیارها) از مجموعه ای از گزینه های موجود است [29]. در ساده ترین حالت، یک مسئله بهینه سازی شامل به حداکثر رساندن یا به حداقل رساندن یک تابع واقعی با انتخاب سیستماتیک مقادیر ورودی از یک مجموعه مجاز و محاسبه مقدار تابع هدف است. در مجموع، تکنیک‌های بهینه‌سازی برای یافتن بهترین راه‌حل برای تابع هدف در حالی که همه محدودیت‌ها برآورده می‌شوند، استفاده می‌شوند [30].از الگوریتم ها می توان نتیجه گرفت که در IDS مبتنی بر ناهنجاری، ویژگی های زیادی برای شناسایی حملات خاص باید در نظر گرفته شود و سیستم باید با حجم عظیمی از ترافیک شبکه مقابله کند. بنابراین تشخیص رفتار عادی در مقابل رفتار غیرعادی چالش ایجاد می‌کند. با ترافیک‌های بزرگ، داده‌های بیشتری باید در هنگام شکل‌گیری الگوها در نظر گرفته شود، که خطر نرخ مثبت کاذب را افزایش می‌دهد. به همین دلیل، بسیاری از محققین از تکنیک یادگیری ماشینی استفاده می کنند و نتایج خروجی نشان می دهد که تکنیک ها می توانند نتایج با دقت بالایی در تشخیص ناهنجاری ها ارائه دهند.

مقدمه

این فصل تکنیک و الگوریتم گذشته و فعلی IDS را توصیف و ارزیابی می کند. ابتدا IDS و تعریف IDS را توضیح داد. سپس شروع به توصیف و مقایسه تکنیک فعلی IDS کنید. نوع IDS و تمرکز محقق را توضیح دهید و اینکه چگونه این نوع IDS می تواند به مدیر کمک کند، چه محدودیتی دارد و چرا محقق این روزها بیشتر بر یادگیری ماشین برای IDS تمرکز می کند. سپس، بررسی چند پروژه مهم در IDS که از یادگیری ماشینی استفاده کرده است، یافتن محدودیت و معیارهای امتیازی برای این پایان نامه. همچنین خلاصه ای از مطالعه تطبیقی تکنیک، روش و الگوریتم موجود بر اساس معیارهای از پیش تعریف شده ارائه شده است. در نهایت، یک رویکرد پیشنهادی برای IDS برای پشتیبانی از امنیت شبکه ارائه می‌کند.

مروری بر IDS

شبکه کامپیوتری یا شبکه داده یک شبکه مخابراتی است که به رایانه ها امکان تبادل داده را می دهد . در شبکه های کامپیوتری، دستگاه های محاسباتی تحت شبکه، داده ها را در طول اتصالات داده به یکدیگر ارسال می کنند. داده ها در قالب بسته ها [31]. اتصالات (پیوندهای شبکه) بین گره ها با استفاده از رسانه کابلی یا رسانه بی سیم برقرار می شود . شناخته شده ترین شبکه کامپیوتری اینترنت [1]. دستگاه های کامپیوتری شبکه ای که داده ها را منشا، مسیریابی و خاتمه می دهند، گره های شبکه نامیده می شوند . گره ها می توانند شامل میزبان هایی مانند رایانه های شخصی c ، تلفن ها ، سرورها و همچنین سخت افزار شبکه [32]. گفته می شود که دو دستگاه از این دست زمانی به هم متصل می شوند که یک دستگاه قادر به تبادل اطلاعات با دستگاه دیگر باشد، خواه ارتباط مستقیمی با یکدیگر داشته باشند یا نه.

تاریخچه اینترنت با توسعه کامپیوترهای الکترونیکی در دهه 1950 آغاز می شود. مفاهیم اولیه in در چندین آزمایشگاه علوم کامپیوتر در ایالات متحده، بریتانیا و فرانسه سرچشمه گرفته است [33]. وزارت دفاع ایالات متحده در اوایل دهه 1960 قراردادهایی را برای سیستم های شبکه بسته منعقد کرد، از جمله توسعه ARPANET (که اولین شبکه ای بود که از اینترنت استفاده می کرد) اولین پیام از طریق ARPANET از آزمایشگاه علوم کامپیوتر پروفسور لئونارد کلاین راک ارسال شد. در دانشگاه کالیفرنیا، لس آنجلس (UCLA) به دومین گره شبکه در موسسه تحقیقاتی استنفورد (SRI) [34].

امنیت شبکه [35]شامل مقررات و خط مشی هایی است که توسط مدیر شبکه برای جلوگیری و نظارت بر دسترسی غیرمجاز، سوء استفاده، اصلاح یا انکار یک شبکه کامپیوتری و منابع قابل دسترسی شبکه اتخاذ می شود. امنیت شبکه شامل مجوز دسترسی به داده ها در یک شبکه است که توسط مدیر شبکه کنترل می شود. کاربران شناسه و رمز عبور یا سایر اطلاعات احراز هویت را انتخاب می کنند یا به آنها اختصاص داده می شود که به آنها امکان دسترسی به اطلاعات و برنامه های تحت اختیار آنها را می دهد [36]. امنیت شبکه انواع شبکه‌های کامپیوتری، عمومی و خصوصی را پوشش می‌دهد که در مشاغل روزمره برای انجام معاملات و ارتباطات بین مشاغل، سازمان‌های دولتی و افراد استفاده می‌شوند. شبکه‌ها می‌توانند خصوصی باشند، مانند داخل یک شرکت، و شبکه‌های دیگری که ممکن است برای دسترسی عمومی باز باشند. امنیت شبکه در سازمان‌ها، شرکت‌ها و انواع دیگر مؤسسات درگیر است [37]. همانطور که عنوانش توضیح می‌دهد این کار را انجام می‌دهد: شبکه را ایمن می‌کند و همچنین بر عملیات‌های انجام شده محافظت و نظارت می‌کند. رایج ترین و ساده ترین راه برای محافظت از یک منبع شبکه با اختصاص یک نام منحصر به فرد و یک رمز عبور مربوط به آن است [38].

در سال 1980، جیمز پی اندرسون مطالعه‌ای را منتشر کرد که در آن راه‌هایی برای بهبود ممیزی و نظارت امنیت رایانه در سایت‌های مشتریان مشخص شد. ایده اصلی پشت شناسه خودکار اغلب به خاطر مقاله‌اش در مورد «چگونگی استفاده از فایل‌های حسابرسی حسابداری برای شناسایی دسترسی‌های غیرمجاز» به او اعتبار داده می‌شود. این مطالعه ID راه را به عنوان شکلی از تشخیص سوء استفاده برای سیستم های اصلی هموار کرد [39]. اولین کار این بود که مشخص کنیم چه تهدیداتی وجود دارد. قبل از طراحی IDS، لازم بود انواع تهدیدها و حملاتی را که می‌توان علیه سیستم‌های رایانه‌ای اعمال کرد و نحوه تشخیص آنها در داده‌های حسابرسی را درک کرد. در واقع، او احتمالاً به نیاز به یک طرح ارزیابی ریسک برای درک تهدید (چه خطرات یا آسیب‌پذیری‌ها، چه حملات ممکن است یا ابزارهای نفوذ) اشاره می‌کرد، بنابراین با ایجاد یک سیاست امنیتی برای محافظت از سیستم های موجود [40].

بین سال های 1984 و 1986، دوروتی دنینگ و پیتر نویمان اولین مدل IDS بلادرنگ را تحقیق و توسعه دادند. این نمونه اولیه سیستم خبره تشخیص نفوذ (IDES) نام گرفت. این IDES در ابتدا یک سیستم خبره مبتنی بر قانون بود که برای شناسایی فعالیت های مخرب شناخته شده آموزش دیده بود. همین سیستم برای شکل دادن به آنچه امروزه به عنوان سیستم خبره تشخیص نفوذ نسل بعدی (NIDES) شناخته می شود، اصلاح و تقویت شده است [41].

گزارش منتشر شده توسط جیمز پی. در این دوره، دولت آمریکا بیشتر این تحقیقات را تامین مالی کرد. پروژه هایی مانند Discovery، Haystack، Multicast Intrusion Detection and Alerting System (MIDAS)، مدیر حسابرسی شبکه و گزارشگر نفوذ (NADIR) همگی برای تشخیص نفوذ توسعه داده شدند [42]. IDS دارای دو نوع سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) و مبتنی بر میزبان (HIDS) است [15]. برخی از سیستم ها ممکن است تلاش کنند تا یک تلاش نفوذ را متوقف کنند اما این نه مورد نیاز است و نه از یک سیستم نظارت انتظار می رود [43].

سیستم های تشخیص نفوذ شبکه

سیستم های تشخیص نفوذ شبکه NIDS در یک نقطه یا نقاط استراتژیک در شبکه قرار می گیرند تا ترافیک به و از همه دستگاه های موجود در شبکه را نظارت کنند [16]. این یک تجزیه و تحلیل برای ترافیک عبوری در کل زیرشبکه انجام می دهد، در حالت بی بند و بار کار می کند، و ترافیکی را که در زیرشبکه ها به کتابخانه حملات شناخته شده منتقل می شود، مطابقت می دهد. هنگامی که حمله شناسایی شد، یا رفتار غیرعادی احساس شد، هشدار می تواند برای مدیر ارسال شود [17]. نمونه ای از NIDS نصب آن بر روی زیرشبکه ای است که فایروال ها در آن قرار دارند تا ببینند آیا کسی در تلاش است به دیوار آتش نفوذ کند یا خیر [18]. در حالت ایده‌آل، می‌توان تمام ترافیک ورودی و خروجی را اسکن کرد، با این حال انجام این کار ممکن است گلوگاهی ایجاد کند که سرعت کلی شبکه را مختل کند [44].

سیستم های تشخیص نفوذ میزبان

سیستم های تشخیص نفوذ میزبان بر روی هاست ها یا دستگاه های موجود در شبکه اجرا می شوند [19]. HIDS بسته‌های ورودی و خروجی را فقط از دستگاه نظارت می‌کند و در صورت شناسایی فعالیت مشکوک به کاربر یا مدیر آن هشدار می‌دهد. یک عکس فوری از فایل های سیستم موجود می گیرد و آن را با عکس فوری قبلی [20]. اگر فایل‌های مهم سیستم اصلاح یا حذف شدند، هشدار برای بررسی به مدیر ارسال می‌شود. نمونه ای از استفاده از HIDS را می توان در ماشین های حیاتی ماموریت مشاهده کرد، که انتظار نمی رود تنظیمات خود را تغییر دهند [21].

IDS دارای دو سیستم برای تشخیص است، غیرفعال و فعال [45]. یک سیستم تشخیص نفوذ فعال (IDS) همچنین به عنوان سیستم تشخیص نفوذ و پیشگیری (IDPS) شناخته می شود. سیستم تشخیص نفوذ و پیشگیری (IDPS) به گونه ای پیکربندی شده است که به طور خودکار حملات مشکوک را بدون هیچ مداخله ای مورد نیاز اپراتور مسدود کند [46]. سیستم تشخیص نفوذ و پیشگیری (IDPS) مزیت ارائه اقدامات اصلاحی بلادرنگ در پاسخ به یک حمله را دارد. IDS غیرفعال سیستمی است که فقط برای نظارت و تجزیه و تحلیل فعالیت ترافیک شبکه پیکربندی شده است و به اپراتور در مورد آسیب پذیری ها و حملات احتمالی هشدار می دهد. IDS غیرفعال به تنهایی قادر به انجام هیچ گونه عملکرد حفاظتی یا اصلاحی نیست [47]دو روش برای تشخیص دارد، IDS مبتنی بر امضا و IDS مبتنی بر ناهنجاری آماری.

IDS مبتنی بر امضا

یک IDS مبتنی بر امضا بسته ها را در شبکه نظارت می کند و آنها را با پایگاه داده امضاها یا ویژگی های تهدیدات مخرب شناخته شده مقایسه می کند [22]. این شبیه به روشی است که اکثر نرم افزارهای آنتی ویروس بدافزار را شناسایی می کنند. مسئله این است که بین یک تهدید جدید که در طبیعت کشف می شود و امضای شناسایی آن تهدید که در IDS شما اعمال می شود فاصله وجود خواهد داشت [48]. در طول آن زمان تاخیر IDS شما قادر به تشخیص تهدید جدید نخواهد بود.

برخی از محبوب‌ترین IDSهای مبتنی بر امضا عبارتند از NFR [49]، Real Secure [50]، Dragon [51]، Snort [52]و Cisco Secure IDS [53]. نشان داده شده است که تشخیص نفوذ مبتنی بر امضا دارای مزایای زیادی مانند پتانسیل نرخ پایین هشدار، دقت تشخیص و گزارش‌های متنی دقیق است. با امضاهای پرمخاطب، شناسایی بسته های مورد علاقه نسبتاً ساده است. به

عنوان مثال، نوشتن یک قانون برای هشدار در تمام بسته های TCP با مجموعه پرچم SYN امری بی اهمیت است. همه IDS ها اجازه توسعه قوانین مستقل را نمی دهند، اما برخی مانند Snort و Dragon قوانین ایجاد شده توسط کاربر را می پذیرند. تقریباً همه فروشندگان IDS قوانینی را برای محصولات خود با تعداد امضاهای متغیر ارائه می کنند که معمولاً در محدوده 500-1500+ قوانین است. قوانین در طول زمان با شناسایی آسیب‌پذیری‌ها و تکنیک‌های اسکن جدید توسط جامعه امنیتی ایجاد می‌شوند. گستردگی و سرعتی که این قوانین توسط فروشنده ایجاد می شوند، معیار خوبی برای اینکه IDS در نهایت چقدر موثر خواهد بود. در حالی که رویکرد مبتنی بر امضا برای تشخیص نفوذ قابل قبول است، اما چیزهای زیادی باقی می ماند. از آنجایی که فروشندگان با امضاهای جدید به صورت هفتگی یا روزانه عرضه می‌شوند، برای یک متخصص امنیتی که از قبل بیش از حد سنگین شده است، به‌روز ماندن با آخرین مجموعه قوانین دشوار است. نقص بسیار جدی‌تر رویکرد IDS مبتنی بر امضا، ناتوانی در شناسایی حملات جدید و ناشناس قبلی است. یک شناسه مبتنی بر امضا فقط به اندازه مجموعه قوانین آن قوی است و اگر حمله جدید باشد، به سادگی هیچ امضایی برای شناسایی کاوشگر ایجاد نخواهد شد. تشخیص نفوذ مبتنی بر امضا نیز توانایی محدودی برای تشخیص اسکن پورت دارد. در واقع، اکثر IDS ها از رویکرد ابتدایی استفاده می کنند، به موجب آن، اگر X رویدادهای مورد علاقه در یک پنجره زمانی به اندازه Y شناسایی شوند [54]، سیستم یک هشدار تولید می کند. با محدود کردن تعداد بسته های هدف در یک شبکه در یک بازه زمانی مشخص، مهاجم می تواند به راحتی از شناسایی توسط IDS فرار کند. این کاستی‌ها در مدل مبتنی بر امضا ذاتی هستند، به همین دلیل است که روش‌های مختلف تشخیص برای رفع نارسایی‌های رویکرد مبتنی بر امضا مورد نیاز است.

IDS مبتنی بر ناهنجاری آماری

یک IDS که مبتنی بر ناهنجاری است، ترافیک شبکه را رصد می کند و آن را با یک خط پایه تعیین شده مقایسه می کند [23]. خط مبنا مشخص می کند که چه چیزی برای آن شبکه "عادی" است - از چه نوع پهنای باندی استفاده می شود، چه پروتکل هایی استفاده می شود، چه پورت ها و دستگاه هایی به طور کلی به یکدیگر متصل می شوند - و در صورت شناسایی ترافیک غیرعادی به مدیر یا کاربر هشدار می دهد. یا به طور قابل توجهی متفاوت از خط پایه است. مسئله این است که اگر خطوط پایه به طور هوشمندانه پیکربندی نشده باشند، ممکن است یک هشدار مثبت کاذب برای استفاده قانونی از پهنای باند به صدا درآورد [24].

سیستم‌های تشخیص نفوذ مبتنی بر آمار (SBIDS) می‌توانند بسیاری از مشکلات ذکر شده IDS مبتنی بر امضا را کاهش دهند. سیستم های مبتنی بر آمار به مدل های آماری مانند قضیه بیز [55]برای شناسایی بسته های غیرعادی در شبکه تکیه می کنند. برای شناسایی یک ناهنجاری، سیستم از داده های جمع آوری شده از رفتار شبکه قبلی استفاده می کند. از آنجایی که هشدارها بر اساس الگوهای استفاده واقعی هستند، سیستم های آماری می توانند با رفتارها سازگار شوند و بنابراین الگوهای استفاده از قوانین خود را ایجاد کنند [56]. الگوهای استفاده چیزی هستند که تعیین می کنند یک بسته چقدر ممکن است برای شبکه غیرعادی باشد. فعالیت غیرعادی توسط تعدادی از متغیرها که در طول زمان نمونه برداری شده و در یک پروفایل ذخیره می شوند اندازه گیری می شود. بر اساس امتیاز ناهنجاری یک بسته، اگر به اندازه کافی غیرعادی باشد، فرآیند گزارش آن را هشدار تلقی می کند. در غیر این صورت، IDS به سادگی ردیابی را نادیده می گیرد [57]. اگر امتیاز ناهنجاری بسته بزرگتر یا مساوی با سطح آستانه تعیین شده توسط کاربر باشد، فرآیند گزارش به کاربر هشدار می دهد. بنابراین، SBIDS الگوها و استفاده از داده های شبکه را شناسایی و ردیابی می کند و سپس یک امتیاز ناهنجاری به هر بسته اختصاص می دهد. پس از انجام این کار، اگر امتیاز ناهنجاری از آستانه

هشدار بیشتر باشد، تسهیلات گزارش دهی یک هشدار تولید می کند [58]. به عنوان مثال، فرض کنید هر روز صبح، شما از خواب بیدار می شوید و روزنامه صبح را می خوانید که بیرون در منتظر است. پس از چند روز یا چند هفته از این رفتار، طبیعی می شود. انتظار دارید که کاغذ صبح به درب منزل برسد. یک روز صبح، روزنامه در آستانه خانه منتظر نیست. در عوض، کاغذ در خیابان خوابیده است. این طبیعی نیست؛ این به وضوح فعالیت غیرعادی است، اما احتمالاً به اندازه ای نیست که تحقیقات را تضمین کند. حال، فرض کنید که شما همچنان شاهد همان الگوی چند کاغذی هستید که هر هفته در خیابان فرود می آیند. سپس، یک روز، شما از خواب بیدار می شوید که اصلاً کاغذی ندارید، یا حتی بدتر از آن، کاغذ از پنجره پرتاب می شود. هیچ یک از این رویدادها عادی نیست، و هر دو نیاز به درجاتی از تحقیقات دارند. اگر یک عدد ناهنجاری با این رویدادها مرتبط باشد، می‌توانیم ببینیم که SBIDS چگونه کار می‌کند. دریافت یک کاغذ در صبح، فعالیت "عادی" تلقی می شود. سیستم الگو را تشخیص می‌دهد و یاد می‌گیرد که این یک رفتار عادی است. سایر فعالیت‌ها بر اساس تعداد رخدادها و میزان "محصول" بودن آنها در رابطه با فعالیت عادی قضاوت می‌شوند [57].

شناسایی الگو اقدامی است برای انجام داده های خام و فعالیت در دسته داده [59]. روش های یادگیری تحت نظارت و بدون نظارت را می توان برای حل مسائل مختلف تشخیص الگو استفاده کرد [60]. در یادگیری نظارت شده، مبتنی بر استفاده از داده های آموزشی برای ایجاد یک تابع است که در آن هر یک از داده های آموزشی شامل یک جفت ورودی است. بردار و خروجی (یعنی برچسب کلاس). وظیفه یادگیری (آموزش) محاسبه فاصله تقریبی بین نمونه های ورودی-خروجی برای ایجاد یک طبقه بندی (مدل) است. وقتی مدل ایجاد می‌شود، می‌تواند نمونه‌های ناشناخته را در برچسب‌های کلاس آموخته‌شده طبقه‌بندی کند [61].

پس از انجام این کار، اگر امتیاز ناهنجاری از آستانه هشدار بیشتر باشد، تسهیلات گزارش دهی یک هشدار تولید می کند [58]. به عنوان مثال، فرض کنید هر روز صبح، شما از خواب بیدار می شوید و روزنامه صبح را می خوانید که بیرون در منتظر است. پس از چند روز یا چند هفته از این رفتار، طبیعی می شود. انتظار دارید که کاغذ صبح به درب منزل برسد. یک روز صبح، روزنامه در آستانه خانه منتظر نیست. در عوض، کاغذ در خیابان خوابیده است. این طبیعی نیست؛ این به وضوح فعالیت غیرعادی است، اما احتمالاً به اندازه ای نیست که تحقیقات را تضمین کند.

حال، فرض کنید که شما همچنان شاهد همان الگوی چند کاغذی هستید که هر هفته در خیابان فرود می آیند. سپس، یک روز، شما از خواب بیدار می شوید که اصلاً کاغذی ندارید، یا حتی بدتر از آن، کاغذ از پنجره پرتاب می شود. هیچ یک از این رویدادها عادی نیست، و هر دو نیاز به درجاتی از تحقیقات دارند. اگر یک عدد ناهنجاری با این رویدادها مرتبط باشد، می‌توانیم ببینیم که SBIDS چگونه کار می‌کند. دریافت یک کاغذ در صبح، فعالیت "عادی" تلقی می شود. سیستم الگو را تشخیص می‌دهد و یاد می‌گیرد که این یک رفتار عادی است. سایر فعالیت‌ها بر اساس تعداد رخدادها و میزان "محصول" بودن آنها در رابطه با فعالیت عادی قضاوت می‌شوند [57].

تحقیقات مرتبط در مورد IDS

طبقه بندی شرح داده شده در زیر به منظور تشکیل سلسله مراتبی است که در جدول 1 نشان داده شده است. یک مشکل کلی این است که اکثر مراجع به صراحت قوانین تصمیم گیری بکار گرفته شده را توصیف نمی کنند، بلکه چارچوبی را که می توان در آن

چنین قوانینی تنظیم کرد. این باعث می شود طبقه بندی تا سطح جزئیاتی که می خواهیم به آن برسیم تقریبا غیرممکن است. بنابراین، ما اغلب باید وقتی به سطح چارچوب، به عنوان مثال سیستم خبره رسیدیم، دسته بندی خود را متوقف کنیم و به این نتیجه برسیم که در حالی که پلت فرم به کار رفته در نقش مشخص شده احتمالاً تأثیر کاملاً مشخصی بر ویژگی های عملیاتی تشخیص نفوذ خواهد داشت. اصل، در حال حاضر نمی‌توانیم دسته‌هایی را تحت تأثیر قرار دهیم. با توجه به این موضوع و این واقعیت که این رشته به عنوان یک کل هنوز به سرعت در حال گسترش است، طبقه بندی فعلی باید به عنوان اولین تلاش در نظر گرفته شود.

از آنجایی که اصطلاحات ثابتی وجود ندارد، ما با مشکل یافتن اصطلاحات رضایت بخش برای طبقات مختلف روبرو هستیم. تا جایی که ممکن است، سعی کرده‌ایم اصطلاحات جدیدی برای پدیده‌هایی که می‌خواهیم توصیف کنیم پیدا کنیم. با این حال، اجتناب از استفاده از عباراتی که قبلاً در این زمینه وجود دارد که اغلب دارای معانی کمی متفاوت هستند یا به طور کلی فاقد تعاریف واضح هستند، ممکن نبوده است. به همین دلیل، ما برای همه اصطلاحات استفاده شده در زیر تعریفی ارائه می دهیم، و مایلیم پیشاپیش از هر گونه سردرگمی که ممکن است پیش بیاید، در صورتی که خواننده قبلاً تعریفی برای یک اصطلاح استفاده شده در ذهن داشته باشد، پوزش می طلبیم.

تشخیص ناهنجاری

ناهنجاری در تشخیص ناهنجاری، ما نه برای نفوذ شناخته شده سیگنال، بلکه به دنبال ناهنجاری در ترافیک مورد نظر هستیم. ما این نگرش را داریم که چیزی که غیر طبیعی است احتمالا مشکوک است. ساخت چنین آشکارساز با ایجاد یک نظر در مورد آنچه که برای موضوع مشاهده شده طبیعی است (که می تواند یک سیستم کامپیوتری، یک کاربر خاص و غیره باشد) شروع می شود، و سپس تصمیم می گیرد که چند درصد از فعالیت را به عنوان غیر طبیعی علامت گذاری کنید، و چگونه برای گرفتن این تصمیم خاص بنابراین، این اصل تشخیص، رفتاری را که بعید است از فرآیند عادی نشات گرفته باشد، بدون توجه به سناریوهای نفوذ واقعی، علامت گذاری می کند.

سیستم های خودآموز

سیستم های خودآموز با مثال می آموزند که چه چیزی برای نصب عادی است. معمولاً با مشاهده ترافیک برای مدت زمان طولانی و ساختن مدلی از فرآیند اساسی. سری های غیرزمانی یک اصطلاح جمعی برای آشکارسازهایی است که رفتار عادی سیستم را با استفاده از یک مدل تصادفی که رفتار سری زمانی را در نظر نمی گیرد، مدل می کند.

مدل‌سازی قوانین خود سیستم ترافیک را مطالعه می‌کند و تعدادی قوانین را تدوین می‌کند که عملکرد عادی سیستم را توصیف می‌کند. در مرحله تشخیص، سیستم قوانین را اعمال می کند و در صورتی که ترافیک مشاهده شده تطابق ضعیفی (به معنای وزنی) با پایه قوانین ایجاد کند، زنگ هشدار را به صدا در می آورد.

آمار توصیفی سیستمی که آمارهای ساده، توصیفی و تک وجهی را از پارامترهای خاص سیستم در یک نمایه جمع آوری می کند و یک بردار فاصله برای ترافیک مشاهده شده و نمایه می سازد. اگر فاصله به اندازه کافی زیاد باشد، سیستم زنگ هشدار را به صدا در می آورد.

سری های زمانی این مدل ماهیت پیچیده تری دارد و رفتار سری زمانی را در نظر می گیرد. به عنوان مثال می توان به تکنیک هایی مانند مدل پنهان مارکوف (HMM)، شبکه عصبی مصنوعی (ANN) و سایر تکنیک های مدل سازی کم و بیش عجیب و غریب مانند یادگیری ماشین اشاره کرد.

یک شبکه عصبی مصنوعی (ANN) نمونه‌ای از رویکرد مدل‌سازی «جعبه سیاه» است. ترافیک عادی سیستم به یک ANN تغذیه می‌شود، که متعاقباً الگوی ترافیک عادی را می‌آموزد. سپس خروجی ANN به ترافیک جدید اعمال می شود و برای تشکیل تصمیم تشخیص نفوذ استفاده می شود. در مورد سیستم بررسی شده، این خروجی از کیفیت کافی برای استفاده برای تشکیل خروجی مستقیم تلقی نمی شد، بلکه به مرحله سیستم خبره سطح دوم که تصمیم نهایی را می گرفت، وارد می شد.

کلاس های برنامه ریزی شده

برنامه‌ریزی‌شده کلاس برنامه‌ریزی‌شده به شخصی نیاز دارد، خواه کاربر باشد یا کارگزار دیگری، که به سیستم آموزش می‌دهد – آن را برنامه‌ریزی می‌کند – تا برخی رویدادهای غیرعادی را شناسایی کند. بنابراین کاربر سیستم در مورد آنچه که به اندازه کافی غیرعادی در نظر گرفته می شود نظر می دهد تا سیستم علامت نقض امنیتی را نشان دهد.

آمار توصیفی این سیستم‌ها با جمع‌آوری آمار توصیفی روی تعدادی از پارامترها، نمایه‌ای از رفتار آماری عادی را با پارامترهای سیستم می‌سازند.

چنین پارامترهایی می تواند تعداد لاگین های ناموفق، تعداد اتصالات شبکه، تعداد دستورات با خطا و غیره باشد.

آمار ساده در همه موارد در این کلاس، آمار جمع‌آوری‌شده توسط مؤلفه‌های سطح بالاتر برای تصمیم‌گیری انتزاعی‌تر برای تشخیص نفوذ استفاده شد.

مبتنی بر قانون ساده، قوانین ساده اما هنوز مرکب را برای اعمال در آمارهای جمع آوری شده به سیستم ارائه می دهد.

آستانه این احتمالاً ساده ترین مثال از آشکارساز آمار توصیفی برنامه ریزی شده است . هنگامی که سیستم آمار لازم را جمع آوری کرد، کاربر می تواند آستانه های از پیش تعریف شده (شاید به شکل محدوده های ساده) را برنامه ریزی کند که تعیین می کند زنگ هشدار را افزایش دهد یا خیر. یک مثال "(Alarm if) تعداد تلاش های ناموفق برای ورود به سیستم است.

پیش‌فرض‌ها انکار می‌کنند ایده این است که به صراحت شرایطی را که تحت آن سیستم مشاهده‌شده به شیوه‌ای امن عمل می‌کند، بیان کنیم و همه انحرافات از این عملیات را به‌عنوان مزاحم علامت‌گذاری کنیم. این مطابقت واضحی با یک سیاست امنیتی انکار پیش‌فرض دارد، که مانند سیستم حقوقی عمومی، موارد مجاز را فرموله می‌کند و هر چیز دیگری را غیرقانونی می‌نامد.

مدل‌سازی سری حالت در مدل‌سازی سری حالت، خط‌مشی عملیات بی‌خطر امنیتی به‌عنوان مجموعه‌ای از حالت‌ها کدگذاری می‌شود. انتقال بین حالت ها در مدل به طور ضمنی است، مانند زمانی که یک ماشین حالت را در یک پوسته سیستم خبره کدگذاری می کنیم، واضح نیست. مانند هر ماشین حالت، هنگامی که با یک حالت مطابقت داشت، موتور سیستم تشخیص نفوذ منتظر می ماند تا

انتقال بعدی رخ دهد. اگر عمل نظارت شده به عنوان مجاز توصیف شود، سیستم ادامه می یابد، در حالی که اگر انتقال سیستم را به حالت دیگری می برد، هر حالت (تلویحی) که به صراحت ذکر نشده باشد باعث می شود سیستم زنگ خطر را به صدا درآورد. اقدامات نظارت شده که می‌توانند انتقال را راه‌اندازی کنند، معمولاً اقدامات مرتبط با امنیت مانند دسترسی به فایل (خواندن و نوشتن)، باز کردن درگاه‌های ارتباطی «ایمن» و غیره هستند.

موتور تطبیق قوانین ساده تر از یک سیستم خبره کامل است و به اندازه آن قدرتمند نیست. مثلاً وحدت وجود ندارد. با این حال، تطبیق فازی را امکان پذیر می‌کند - به این معنا که ویژگی‌هایی مانند «دسترسی به هر فایلی در دایرکتوری /tmp» می‌تواند یک انتقال را راه‌اندازی کند، مبهم است. در غیر این صورت، مشخصات واقعی عملیات بی خطر امنیتی برنامه احتمالاً نمی تواند به صورت واقع بینانه انجام شود.

تشخیص امضا

امضا در تشخیص امضا، تصمیم تشخیص نفوذ بر اساس دانش مدلی از فرآیند نفوذی و اینکه چه ردپایی باید در سیستم مشاهده شده باقی بگذارد، شکل می‌گیرد. ما می‌توانیم در همه موارد تعریف کنیم که چه چیزی رفتار قانونی یا غیرقانونی است و رفتار مشاهده‌شده را بر این اساس مقایسه کنیم.

لازم به ذکر است که این آشکارسازها سعی می کنند شواهدی از فعالیت های نفوذی را بدون توجه به اینکه ترافیک پس زمینه، یعنی رفتار عادی سیستم به چه صورت است، شناسایی کنند.

این آشکارسازها باید بتوانند بدون توجه به رفتار عادی سیستم عمل کنند و در عوض به دنبال الگوها یا سرنخ هایی باشند که توسط طراحان تصور می شود در مقابل ترافیک پس زمینه احتمالی متمایز باشند. این خواسته های بسیار دقیقی را در مورد مدل ماهیت نفوذ ایجاد می کند. اگر قرار باشد آشکارساز حاصل از تشخیص و نرخ هشدار نادرست قابل قبولی برخوردار باشد، در اینجا نمی توان شلختگی را در نظر گرفت.

برنامه ریزی شده این سیستم با یک قانون تصمیم گیری صریح برنامه ریزی شده است، جایی که برنامه خودش از نفوذ کانال بر فضای مشاهده سود برده است.قانون تشخیص ساده است به این معنا که شامل یک کدگذاری ساده از آنچه می توان انتظار داشت در صورت نفوذ مشاهده شود، است.

بنابراین، ایده این است که به صراحت بگوییم چه ردپایی از نفوذ می تواند به طور منحصر به فرد در فضای مشاهده رخ دهد. این مطابقت واضحی با یک خط مشی امنیتی مجوز پیش فرض، یا فرمولی که در قانون رایج است، دارد، یعنی فهرست کردن رفتارهای غیرقانونی و در نتیجه تعریف همه مواردی که به صراحت در فهرست مجاز نیستند.

مدل‌سازی حالت، نفوذ را به‌عنوان تعدادی حالت مختلف رمزگذاری می‌کند، که هر کدام باید در فضای مشاهده حضور داشته باشند تا نفوذ رخ داده در نظر گرفته شود. آنها طبیعتاً مدل های سری زمانی هستند. دو زیر کلاس وجود دارد: در مرحله اول، انتقال حالت، حالت هایی که نفوذ را تشکیل می دهند، زنجیره ساده ای را تشکیل می دهند که باید از ابتدا تا انتها طی شود. در دومی، شبکه

پتری، ایالت ها شبکه پتری را تشکیل می دهند. در این مورد، آنها می توانند ساختار درختی کلی تری داشته باشند، که در آن چندین حالت آماده سازی می توانند به هر ترتیبی انجام شوند، صرف نظر از اینکه در کجای مدل رخ می دهند.

سیستم خبره یک سیستم خبره برای استدلال در مورد وضعیت امنیتی سیستم، با توجه به قوانینی که رفتار مداخله جویانه را توصیف می کند، استفاده می شود. اغلب از ابزارهای مبتنی بر تولید زنجیره‌ای رو به جلو استفاده می‌شود، زیرا این ابزارها هنگام برخورد با سیستم‌هایی که در آن حقایق جدید (رویدادهای حسابرسی) دائماً وارد سیستم می‌شوند، مناسب‌ترین هستند.

این سیستم‌های خبره اغلب از قدرت و انعطاف‌پذیری قابل‌توجهی برخوردارند و به کاربر اجازه دسترسی به مکانیسم‌های قدرتمندی مانند یکپارچه‌سازی را می‌دهند. این اغلب در مقایسه با روش‌های ساده‌تر هزینه‌ای برای سرعت اجرا دارد.

تطبیق رشته یک تطبیق ساده، اغلب حساس به حروف کوچک، زیر رشته کاراکترهای متن است که بین سیستم ها منتقل می شود، یا در غیر این صورت از استفاده از سیستم ناشی می شود. چنین روشی البته به هیچ وجه انعطاف پذیر نیست، اما این فضیلت را دارد که درک آن ساده باشد. بسیاری از الگوریتم‌های کارآمد برای جستجوی زیر رشته‌ها در یک رشته طولانی‌تر (رویداد حسابرسی) وجود دارد.مبتنی بر قوانین ساده شبیه به سیستم‌های خبره قدرتمندتر هستند، اما نه به اندازه پیشرفته‌تر. این اغلب منجر به اجرای سریعتر می شود.

آشکارسازهای مرکب

امضا الهام گرفته از این آشکارسازها یک تصمیم ترکیبی را با توجه به مدلی از رفتار عادی سیستم و رفتار نفوذی مزاحم تشکیل می دهد. آشکارساز با تشخیص نفوذ در پس زمینه ترافیک عادی در سیستم عمل می کند. در حال حاضر، ما این آشکارسازها را "امضا الهام گرفته شده" می نامیم زیرا مدل نفوذی بسیار قوی تر و واضح تر از مدل معمولی است. این آشکارسازها - حداقل در تئوری - شانس بسیار بیشتری برای تشخیص صحیح رویدادهای واقعاً جالب در سیستم نظارت شده دارند، زیرا هم الگوهای رفتار نفوذی را می شناسند و هم می توانند آنها را با رفتار عادی سیستم مرتبط کنند.

این آشکارسازها حداقل می‌توانند تصمیمات خود را بهتر ارزیابی کنند، یعنی به ما نشانه بهبودیافته‌ای از کیفیت زنگ هشدار بدهند. بنابراین این سیستم ها از برخی جهات پیشرفته ترین آشکارسازهای بررسی شده هستند که چه چیزی برای یک سیستم رفتار مزاحم و عادی را تشکیل می‌دهد و با ارائه نمونه‌هایی از رفتار عادی همراه با رفتار مزاحم می‌آید. بنابراین، نمونه‌های رفتار مداخله جویانه باید توسط برخی از مقامات خارجی به عنوان چنین پرچم‌گذاری شوند تا سیستم بتواند این دو را از هم متمایز کند. انتخاب خودکار ویژگی تنها یک نمونه از چنین سیستمی در این طبقه بندی وجود دارد و با تعیین خودکار ویژگی های قابل مشاهده در هنگام تشکیل تصمیم تشخیص نفوذ جالب، جداسازی آنها و استفاده از آنها برای تشکیل تصمیم تشخیص نفوذ بعدا عمل می کند.

منابع

1. Grobstein, D.L., and Uhlig, R.P.: 'A wholesale retail concept for computer network management', in Editor (Ed.)^(Eds.): 'Book A wholesale retail concept for computer network 898-889 .edn.), pp ,1972 ,management' (ACM

2. Internet Crime 2013 Internet Crime Report', in Editor (Ed.)^(Eds.): 'Book 2013' :.Center, I.C.C .edn.), pp ,2013) 'Report

3. Jajodia, S., Noel, S., and O'Berry, B.: 'Topological analysis of network attack vulnerability': 266-247 .pp ,(2005 ,Managing Cyber Threats' (Springer'

4. Santiraveewan, V., and Permpoontanalarp, Y.: 'A graph-based methodology for analyzing ip spoofing attack', in Editor (Ed.)^(Eds.): 'Book A graph-based methodology for analyzing ip 230-227 .edn.), pp ,2004 ,spoofing attack' (IEEE

5. Hunt, R.: 'Internet/Intranet firewall security—policy, architecture and transaction services', 1123-1107 .pp ,(13) ,21 ,1998 ,Computer Communications

6. Cheswick, W.R., and Whitten, E.G.: 'Firewall security method and apparatus', in Editor .edn.), pp ,2001 ,(Ed.)^(Eds.): 'Book Firewall security method and apparatus' (Google Patents

7. Baum, R.T., Eggerl, E.M., Burton, W.R., and Cloutier, L.C.: 'Real time firewall security', in .edn.), pp ,2002 ,Editor (Ed.)^(Eds.): 'Book Real time firewall security' (Google Patents

8. Feng, G., and Hughes, J.: 'Analyzing privacy and security issues in the information age–An ,(1) ,6 ,2009 ,ethical perspective', WSEAS Transactions on Information Science and Applications 135-126 .pp

9. Ehlert, S., Zhang, G., and Magedanz, T.: 'Increasing SIP firewall performance by ruleset size limitation', in Editor (Ed.)^(Eds.): 'Book Increasing SIP firewall performance by ruleset size 6-1 .edn.), pp ,2008) 'limitation

10. Hughes, W.: 'Systems and methods for intelligent monitoring and response to network threats', in Editor (Ed.)^(Eds.): 'Book Systems and methods for intelligent monitoring and .edn.), pp ,2006 ,response to network threats' (Google Patents

11. Roesch, M.: 'Snort: Lightweight Intrusion Detection for Networks', in Editor (Ed.)^(Eds.): 238-229 .edn.), pp ,1999) 'Book Snort: Lightweight Intrusion Detection for Networks'

12. Smaha, S.E.: 'Haystack: An intrusion detection system', in Editor (Ed.)^(Eds.): 'Book 44-37 .edn.), pp ,1988 ,Haystack: An intrusion detection system' (IEEE

13. in Editor (Ed.)^(Eds.): 'Book Global ,'2013 : Lab, K.: 'Global Corporate IT Security Risks .edn.), pp ,2013) '2013 : Corporate IT Security Risks

14. Shaveta, E., Bhandari, A., and Saluja, K.K.: 'Applying Genetic Algorithm in Intrusion 2014 ,'Detection System: A Comprehensive Review

15. 7-3 .pp ,(4) ,2 ,1996 ,Sundaram, A.: 'An introduction to intrusion detection', Crossroads

16. Wang, K., and Stolfo, S.J.: 'Anomalous payload-based network intrusion detection', in Editor ,2004 ,(Ed.)^(Eds.): 'Book Anomalous payload-based network intrusion detection' (Springer 222-203 .edn.), pp

17. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., and Vázquez, E.: 'Anomaly-,based network intrusion detection: Techniques, systems and challenges', computers & security 28-18 .pp ,(1) ,28 ,2009
18. Chen, T., and Sun, M.: 'Network intrusion detection system', in Editor (Ed.)^(Eds.): 'Book .edn.), pp ,2009 ,Network intrusion detection system' (Google Patents
19. ,de Boer, P., and Pels, M.: 'Host-based intrusion detection systems', Amsterdam University 2005
20. Vokorokos, L., and Baláž, A.: 'Host-based intrusion detection system', in Editor (Ed.)^(Eds.): 36-32 .edn.), pp ,2010 ,Book Host-based intrusion detection system' (IEEE Press'
21. Kothari, S., Parmar, H., Das, E., Panda, N., Ahmed, A., and Marchang, J.: 'Host Based Intrusion Detection System', in Editor (Ed.)^(Eds.): 'Book Host Based Intrusion Detection .edn.), pp ,2011 ,System' (ASME Press
22. Kruegel, C., and Toth, T.: 'Using decision trees to improve signature-based intrusion detection', in Editor (Ed.)^(Eds.): 'Book Using decision trees to improve signature-based 191-173 .edn.), pp ,2003 ,intrusion detection' (Springer
23. Depren, O., Topallar, M., Anarim, E., and Ciliz, M.K.: 'An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks', Expert systems with 722-713 .pp ,(4) ,29 ,2005 ,Applications
24. .2011 ,Whitman, M., and Mattord, H.: 'Principles of information security' (Cengage Learning (2011
25. Axelsson, S.: 'Intrusion detection systems: A survey and taxonomy', in Editor (Ed.)^(Eds.): .edn.), pp ,2000 ,Book Intrusion detection systems: A survey and taxonomy' (Technical report'
26. Kalekar, A., Kshatriya, N., Chakranarayan, S., and Wadekar, S.: 'Real Time Intrusion Detection System using Machine Learning', in Editor (Ed.)^(Eds.): 'Book Real Time Intrusion .edn.), pp ,2014 ,Detection System using Machine Learning' (ESRSA Publications
27. Münz, G., Li, S., and Carle, G.: 'Traffic anomaly detection using k-means clustering', in Editor .edn.), pp ,2007) '(Ed.)^(Eds.): 'Book Traffic anomaly detection using k-means clustering
28. Dönmez, P.: 'Introduction to Machine Learning, by Ethem Alpaydın. Cambridge, MA: The pages', Natural Language 584 +39.95 £/54$ .0-01243-262-0-978 :ISBN .2010 MIT Press 288-285 .pp ,(02) ,19 ,2013 ,Engineering
29. Aickelin, U., Greensmith, J., and Twycross, J.: 'Immune system approaches to intrusion 329-316 .pp ,(2004 ,detection–a review': 'Artificial Immune Systems' (Springer
30. Abadeh, M.S., Habibi, J., and Lucas, C.: 'Intrusion detection using a fuzzy genetics-based 428-414 .pp ,(1) ,30 ,2007 ,learning algorithm', Journal of Network and Computer Applications
31. Roberts, L.G., and Wessler, B.D.: 'Computer network development to achieve resource sharing', in Editor (Ed.)^(Eds.): 'Book Computer network development to achieve resource 549-543 .edn.), pp ,1970 ,sharing' (ACM
32. ,Wegner, D.M.: 'A computer network model of human transactive memory', Social cognition 339-319 .pp ,(3) ,13 ,1995

33. Mowery, D.C., and Simcoe, T.: 'Is the Internet a US invention?—an economic and technological history of computer networking', Research Policy ,2002 ,31 ,(8) .pp 1369-1387
34. Salus, P.H., and Vinton, G.: 'Casting the Net: From ARPANET to Internet and Beyond' (Addison-Wesley Longman Publishing Co., Inc ,.1995 .1995)
35. Simmonds, A., Sandilands, P., and Van Ekert, L.: 'An ontology for network security attacks': Applied Computing' (Springer' ,2004) .pp 317-323
36. Kaufman, C., Perlman, R., and Speciner, M.: 'Network security: private communication in a public world' (Prentice Hall Press ,.2002 .2002)
37. Stallings, W.: 'Network and internetwork security: principles and practice' (Prentice Hall Upper Saddle River, NJ ,.1995 .1995)
38. Forouzan, B.A.: 'Cryptography & Network Security' (McGraw-Hill, Inc ,.2007 .2007)
39. Anderson, J.P.: 'Computer security threat monitoring and surveillance', in Editor (Ed.)^(Eds.): Book Computer security threat monitoring and surveillance' (Technical report, James P. ' .edn.), pp ,1980 ,Anderson Company, Fort Washington, Pennsylvania
40. Lunt, T.F., Tamaru, A., Gilham, F., Jagannathan, R., Jalali, C., Neumann, P.G., Javitz, H.S., Valdes, A., and Garvey, T.D.: 'A real-time intrusion-detection expert system (IDES)' (SRI International, Computer Science Laboratory ,.1992 .1992)
41. Denning, D.E., and Neumann, P.G.: 'Requirements and model for IDES—a real-time intrusion detection expert system', Document A005 ,SRI International ,1985 ,333
42. Bace, R.G.: 'Intrusion detection' (Sams Publishing ,.2000 .2000)
43. Mukherjee, B., Heberlein, L.T., and Levitt, K.N.: 'Network intrusion detection', Network, IEEE ,1994 ,8 ,(3) .pp 26-41
44. Cao, C.-M., Chen, T., Liu, W.-H., Ma, C.-M., and Meng, C.: 'Network intrusion detection system', in Editor (Ed.)^(Eds.): 'Book Network intrusion detection system' (Google Patents ,2008 .edn.), pp
45. Freedman, J., Ivory, C.J., and Wu, H.: 'Network intrusion detection and analysis system and method', in Editor (Ed.)^(Eds.): 'Book Network intrusion detection and analysis system and method' (Google Patents ,2009 .edn.), pp
46. Biermann, E., Cloete, E., and Venter, L.M.: 'A comparison of intrusion detection systems', Computers & Security ,2001 ,20 ,(8) .pp 676-683
47. Desai, A., Jiang, Y., Oliveto, J., and Tarkington, W.: 'Multi-level and multi-platform intrusion detection and response system', in Editor (Ed.)^(Eds.): 'Book Multi-level and multi-platform intrusion detection and response system' (Google Patents ,2002 ,intrusion .edn.), pp
48. McHugh, J., Christie, A., and Allen, J.: 'The role of intrusion detection systems', Washington Post ,2000
49. احمد, ه., and آیدا, ه.: 'استفاده از روش های بیوانفورماتیک و سیتوژنتیک مولکولی در بررسی ناهنجاریهای کروموزومی سلول های سرطان پوست القائی در رت های نژاد SD', 2020
50. realsecure.html/1-http://www.checkpoint.com/products/firewall
51. http://www.portcullis-security.com/products/index.htm
52. http://www.snort.org

53. /http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz
54. Stephen, N., and Novak, J.: 'Network Intrusion Detection, An Analyst's Handbook', Beijing: 219-207 .pp ,2000 ,Peoples Posts & Telecommunications Publishing House
55. (1993 .1993 ,Lupton, R.: 'Statistics in theory and practice' (Princeton University Press
56. Bass, T.: 'Intrusion detection systems and multisensor data fusion', Communications of the 105-99 .pp ,(4) ,43 ,2000 ,ACM
57. 1994 ,'Kumar, S., and Spafford, E.H.: 'A pattern matching model for misuse intrusion detection
58. Yeung, D.-Y., and Ding, Y.: 'Host-based intrusion detection using dynamic and static 243-229 .pp ,(1) ,36 ,2003 ,behavioral models', Pattern recognition
Michalski, R.S., Bratko, I., and Bratko, A.: 'Machine learning and data mining; methods and .59 (1998 .1998 ,.applications' (John Wiley & Sons, Inc
60. Li, X.-B.: 'A scalable decision tree system and its application in pattern recognition and 130-112 .pp ,(1) ,41 ,2005 ,intrusion detection', Decision Support Systems
61. Tsai, C.-F., Hsu, Y.-F., Lin, C.-Y., and Lin, W.-Y.: 'Intrusion detection by machine learning: 12000-11994 .pp ,(10) ,36 ,2009 ,A review', Expert Systems with Applications

A comprehensive overview of intrusion detection system techniques

Amin Dastanpour

Department of Computer Engineering, Kerman Institute of Higher Education
amindastanpoure@gmail.com

Abstract - A data network or a computer network is a telecommunication network in which computers are used to exchange data. The form of data conversion is called packet, wireless media or cable media are used to create links in the network (connections) between nodes. The Internet is known as the most popular computer network. In computer networks, an attack is defined as any attempt to destroy, disclose, alter, disable, steal, gain unauthorized access to, or use an asset. It shows the classification of attackers, which are divided into two categories: external and internal attackers. An external attacker is an external attack, where someone from outside the network tries to bypass or penetrate secure systems. Outline of the foreign attacker in order to prevent the attacks of this type of attacker, scientists suggest using a firewall. Network security is defined as controlling incoming and outgoing network traffic based on a set of applied rules. A firewall places a barrier between a trusted and secure internal network and other networks (eg the Internet) that are assumed to be untrusted and secure. The major problem with firewall is that it cannot protect the network from internal attackers. In other words, a firewall does not have the ability to prevent individual users who use modems to dial in or out of the network and the attack bypasses the firewall. To prevent the attacks of these types of attackers, the administrator uses the intrusion detection system. An intrusion detection system (IDS) is a device or software that monitors network or system activity for malicious activity or policy violations and provides reports to a management station. In addition, a firewall can block a connection, while an intrusion detection system (IDS) cannot block a connection and only reports any intrusion attempts to the security manager. warns in this article, it states the importance of intrusion detection and checking its types, in addition to checking its techniques.

Keywords: review, network security, intrusion detection system, network security techniques, IDS intrusion detection system