7th Conference on Recent Research in Science and Technology
هفتمین همایش پژوهش های نوین در علوم و فناوری
پاییز ۱۳۹۵
Autumn 2016

تشخیص نفوذ به شبکه با استفاده از تکنیک های داده کاوی

سیدحسین قریشی[۱]
دانشجوی کارشناسی ارشد فناوری اطلاعات تجارت الکترونیک ، موسسه آموزش عالی مهر آستان ، گیلان ، ایران
sh.ghoreyshi@gmail.com

اعظم عندلیب[۲]
عضوهیات علمی گروه مهندسی کامپیوتر ، واحد رشت ، دانشگاه آزاد اسلامی ، رشت ، گیلان ، ایران
Azam.andalib@gmail.com

چکیده:

داده‌کاوی (به انگلیسی: Data Mining) به مفهوم استخراج اطلاعات نهان و یا الگوها وروابط مشخص در حجم زیادی از داده‌ها در یک یا چند بانک اطلاعاتی بزرگ است. داده‌کاوی پایگاه‌ها و مجموعه‌های حجیم داده‌ها را در پی کشف واستخراج دانش، مورد تحلیل و کند و کاوهای ماشینی (و نیمه‌ماشینی) قرار می‌دهد. این گونه مطالعات و کاوش‌ها را به واقع می‌توان همان امتداد و استمرار دانش کهن و همه جا گیر آمار دانست. تفاوت عمده در مقیاس، وسعت و گوناگونی زمینه‌ها و کاربردها، و نیز ابعاد و اندازه‌های داده‌های امروزین است که شیوه‌های ماشینی مربوط به یادگیری، مدل‌سازی، و آموزش را طلب می‌نماید.

یکی از موضوعاتی که امروزه در داده کاوی مطرح است، نفوذ به شبکه های کامپیوتری و پایگاههای اطلاعاتی می باشد که در حال حاضر جزء مباحث مهم و روزمره این حوزه می باشد.

به منظور مقابله نفوذ کنندگان به شبکه ها و سیستم های کامپیوتری روش های متعددی تدوین شده است که روشهای تشخیص نفوذ نامیده می شود.بر اساس این روشها سیستم های متعددی تحت عنوان سیستم های تشخیص نفوذ طراحی و ساخته شده اند. سیستم‌های تشخیص نفوذ (IDS) وظیفه‌ی شناسایی و تشخیص هر گونه سوء استفاده و یا آسیب‌رسانی توسط هر دو دسته‌ی کاربران داخلی و خارجی را با استفاده از قوانین داده کاوی بر عهده دارند ، همچنین این تشخیص نوعی جلوگیری نیز به شمار می رود.

کلمات کلیدی: **داده‌کاوی، سیستم‌های تشخیص نفوذ، روشهای تشخیص نفوذ، شبکه های کامپیوتری**

۱. مقدمه:

داده کاوی، استخراج داده از منابع عظیم داده است تا اطلاعات گرانبهایی که در حجم انبوهی از اطلاعات پنهان شده است را استخراج کند. داده کاوی ترجمه ی عبارتData Mining و به معنای کاویدن معادن داده است .برای انجام عملیات داده کاوی قبل از هرچیزی بایدبر روی داده ها عمل پیش پردازش انجام گیرد.سیستم های تشخیص نفوذ به عنوان یکی از عناصر اصلی زیرساخت های امنیت در بسیاری از سازمانها می باشند.این سیستم ها ، مدل ها و الگوهای سخت افزاری و نرم افزاری می باشند که به خودکار کردن فرآیندهایی می پردازد.

فایروال (دیوار آتش و یا برابر فرهنگستان زبان: بارو) نام عمومی برنامه‌هایی است که از دستیابی غیرمجاز به یک سیستم رایانه جلوگیری می‌کنند. در برخی از این نرم‌افزارها، برنامه‌ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه‌ها، داده ارسال کنند.

یکی از کاربردهای معمول فایروال واگذاری اختیار ویژه به گروهی خاص از کاربران جهت استفاده از یک منبع بوده، و همچنین بازداشتن کسانی که از خارج از گروه خواهان دسترسی به منبع هستند می‌باشد. استفاده دیگر فایروال جلوگیری از ارتباط مستقیم یک سری از رایانه‌ها با دنیای خارج می‌باشد. هر چند فایروال بخش مهمی از سیستم امنیتی را تشکیل می‌دهد ولی طراحان به این نکته نیز توجه می‌ورزند که اکثر حملات از درون شبکه می‌آیند و نه از بیرون آن.

این قسمت با معرفی سیستم های تهاجم یاب یا IDS به بررسی چگونگی محافظت از شبکه در مقابل حملاتی که فایروال قادر به تشخیص آنها نمی باشد می پردازد.

سیستم های تهاجم یاب نرم افزارهایی هستند که با بررسی ترافیک شبکه و از روی یک سری نشانه ها این حمالات را تشخیص می دهند. این نوع سیستم ها در کنار فایروال و برای ایجاد امنیت بیشتر بکار می روند. یک سیستم تهاجم یاب می تواند فقط از یک سیستم و یا از تمامی سیستم های موجود در شبکه محافظت کند که درحالت دوم NIDS نامیده می شود . نحوه ی برخورد سیستم های تهاجم یاب در قبال موارد مشکوک و حمالات آنها را به دو دسته ی فعال و انفعالی تقسیم می کند . سیستم های تهاجم یاب فعال می توانند طوری برنامه ریزی شوند که به محض بروز یک مورد مشکوک عکس العمل مناسب نشان دهند (قطع ارتباط مشکوک، تولیدیک هشدار ، ...) ولی سیستم های تهاجم یاب انفعالی فقط اتفاقات رخ داده را ثبت می کنند که بعداً می توانند مورد بررسی قرار گیرند.

تشخیص نفوذ:

با رشد سریع اینترنت مشکلات مربوط به آن نیز افزایش یافته است علاوه بر این تکنولوژی نفوذ به سمت روشهای پیچیده ای چون حملات هماهنگ و مشارکتی سوق پیدا کرده است .در چنین شرایطی نیاز مبرم به ابزارهای نرم افزاری که بتوانند به طور خودکار دامنه وسیعی از نفوذها را شناسایی کنند ، احساس می شود .سیستمهای تشخیص نفوذ به عنوان نگهبان شبکه باید توانایی شناسایی و دفاع را در زمان بسیار کوتاه داشته باشند .در یک دسته بندی کلی می توان سیستمهای تشخیص نفوذ را به سیستمهای متمرکز و توزیع تقسیم بندی نمود .در سیستم های متمرکز تمام اجزاء سیستم تشخیص نفوذ به صورت یکجا و بر روی یک رسانه در شبکه فعالیت می کنند.

در سیستم های توزیع شده با هدف افزایش ضریب ایمنی،تحمل پذیرآسیب و توزیع بار ترافیکی شبکه تمام یا برخی از اجزاء

سیستم تشخیص نفوذ مانند حسگرها ،واقع نگار و یا حتی جزء تحلیلگر بر روی ناحیه های مختلف یک شبکه یا چندین شبکه متفاوت توزیع می شوند.

فرآیند نفوذ:

به طور کلی نفوذ و حمله از جانب نفوذی به شبکه های کامپیوتری در طی سه مرحله به شبکه صورت می گیرد:

- شناسایی
- یافتن نقاط ضعف سیستم و بدست آوردن سناریوی نفوذ
- حمله و نفوذ

همانگونه که سیستم های کامپیوتری مبتنی بر شبکه نقش حیاطی رو به رشدی را در جوامع امروزی ایفا می کنند توسط دشمنان و مجرمین ، آماج نفوذ ها و حملات بیشتری قرار میگیرند.

علاوه بر روش های جلوگیری از نفوذ[1] از قبیل تصدیق اصالت کاربر مانند استفاده از کلمات رمز، استفاده از دیواره های آتش و محافظت از اطلاعات مانند رمزنگاری از تشخیص نفوذ نیز به عنوان دیوار دیگری برای محافظت از شبکه های کامپیوتری استفاده می شود.

هدف ازتشخیص نفوذ این است که استفاده غیرمجاز ، سوء استفاده و آسیب رساندن به سیستم ها و شبکه های کامپیوتری توسط هر دو دسته کاربران داخلی و حمله کنندگان خارجی شناسایی شود.

به منظور پیاده سازی روشهای تشخیص نفوذ سیستم های متعددی تحت عنوان سیستمهای تشخیص نفوذ[2] طراحی و ساخته شده اند.در حوزه امنیت کامپیوتر ، سیستم های تشخیص نفوذ نقش هشدار دهنده را ایفا می کنند و هر زمان که امنیت سایت[3] در معرض خطر قرار می گیرد آن را اعلام می کنند.نهاد دیگری که مسئول امنیتی سایت نامیده می شود،می تواند به این هشدارها پاسخ داده و احکام مناسب را انجام دهد.

سیستم تشخیص نفوذ:

در طی چند سال گذشته چندین نوع متفاوت از سیستم های تشخیص نفوذ ساخته شده اند.سیستم های تشخیص نفوذ اولیه با تحلیل فایلهای رخدادها[4] که توسط سیستم عامل و برنامه های کاربردی ایجاد می شوند،کار می کردند اما به مرور که این سیستم های پیچیده شدند به داده های کافی برای شناسایی کامل یک حمله دسترسی نداشتند بنابراین توجه به روشهای تشخیص نفوذ پیچیده تر مبتنی بر تحلیل داده های شبکه یا میزبان معطوف شد بر اساس منبع اطلاعات دریافتی تشخیص نفوذ به سه دسته تقسیم می شوند که عبارتند از:

۱. سیستم های تشخیص نفوذ مبتنی بر میزبان
۲. سیستم های تشخیص نفوذ مبتنی بر شبکه
۳. سیستم های تشخیص نفوذ توزیع شده

---

[1] Intrusion Prevention
[2] IDS(Intrusion Detection System)

[3] Site Security Offer
[4] Log files

تشخیص و جلوگیری از نفوذ سه وظیفه جمع آوری داده ها،آنالیز داده ها و عملیات پاسخ را شامل می شود.در بخش جمع آوری داده ها سیستم ،اطلاعات مورد نیاز خود را مانند دسترسی به فایلهای مختلف تحت نظارت و یا اطلاعات در مورد عملکرد شبکه،جمع آوری می کند. در سیستم های مبتنی بر میزبان ، داده ها بر اساس منابع داخل میزبان که اکثرا در سطح سیستم عامل می باشند جمع آوری می شود. از سوی دیگر در سیستم های مبتنی بر شبکه با آنالیز بسته های عبوری در شبکه پارامترهای مورد نیاز جهت تشخیص نفوذدر اختیار بخش آنالیز قرار می گیرند.تعیین دقیق داده هایی که باید جمع آوری شوند وسیله ای حساس در عملکرد تشخیص نفوذ است.اکثر سیستم های عامل ، رویدادهای مرتبط با امنیت را جمع آوری می کنند که می تواند منبع اطلاعات خوبی برای تشخیص نفوذ باشد اما این رویدادها در بیشتر مواقع اطلاعات ساده ای نظیر دفعات خطا در ورود به سیستم ویا تلاش برای دسترسی به منابع غیرمجاز توسط کاربران را ارائه می کنند این اطلاعات جهت تشخیص حملاتی که با سناریوهای پیچیده و استفاده از اختیارات مجاز یک کاربر انجام می شوند،چندان مفید نیست بنابراین سیستم های تشخیص نفوذ علاوه بر استفاده از رویدادهای سیستم های مورد نظارت حسگرهایی را جهت جمع آوری داده های مورد نیازشان به کار می گیرند.این حسگرها ممکن است در یک میزبان به بررسی جوانب مختلف عملیات سیستم بپردازند و یا در یک معماری توزیع شده در نقاط مختلف شبکه و میزبان های محیط تخت نظارت خود قرار بگیرد.با پیچیده تر شدن سناریوهای حملات ،حجم اطلاعاتی که لازم است تا حسگرها جمع آوری کنند افزایش می یابد. این مسئله نه تنها باعث پیچیدگی آنالیز داده ها می گردد بلکه مسئله دیگری تحت عنوان ذخیره سازی و بازیابی سریع اطلاعات را مطرح می کند.[2]

داده کاوی و تشخیص نفوذ:

در یک پروژه تشخیص نفوذ قسمتهای خاص از داده کاوی مورداستفاده قرار می گیردکه به صورت زیر هستند:

- حذف کردن داده های نرمال از داده های مشکوک به حمله که به تحلیلگران اجازه تمرکز بیشتر برای یافتن حمله های واقعی را می دهد.
- تشخیص تولیدکنندگان اعلان های غلط.
- یافتن فعالیتهای غیرعادی که باعث آشکار شدن حمله های واقعی می شوند.
- تشخیص الگوها،تشخیص آدرسهای IP و فعالیتهای مشابه.

برای انجام این فعالیتها ،داده کاوان از روشهای زیر استفاده می کنند:

- خلاصه سازی داده ها توسط آمارها،یافتن مقادیر خارج از محدوده.
- آشکار سازی ارائه خلاصه گرافیکی از داده ها.
- خوشه سازی داده ها در دسته های طبیعی.
- کشف قواعد وابستگی تعریف فعالیتهای عادی و فعال ساختن کشف موارد غیرعادی.
- دسته بندی:پیشگویی کردن دسته هایی که در برگیرنده رکوردهای خاص هستند.

سیستم های تشخیص نفوذ مبتنی بر داده کاوی به دو بخش تقسیم می شوند.

اولی کشف سوء استفاده[5] و دومی تشخیص رفتار غیرعادی(کشف آنومالی[6]) می باشد. در سیتم های کشف سوء استفاده به ساخت الگوهای نفوذ با استفاده از یادگیری از داده های برچسب گذاری شده[7] پرداخته می شود.در این مدل سیستم نمی تواند به شناسایی حملات جدید بپردازد ولی در مقابل،سیستم های تشخیص رفتار غیرعادی می توانند به شناسایی نفوذهای جدید و ناشناخته بپردازند[3].

در این روش ، یک نما از رفتار عادی ایجاد می شود.یک ناهنجاری ممکن است نشاندهنده یک نفوذ باشد برای ایجاد نماهای رفتار عادی از رویکردهایی از قبیل شبکه های عصبی ، تکنیک های یادگیری ماشین و غیره استفاده می شود.برای تشخیص رفتار غیرعادی ، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آنها پیدا کرد.رفتارهایی که از این الگوها پیروی می کنند،عادی بوده و رویدادهایی که انحرافی بیش از حد معمول آماری از این الگوها دارند،به عنوان رفتار غیرعادی تشخیص داده می شود.

نفوذهای غیرعادی برای تشخیص بسیار سخت هستند،چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد.معمولا رویدادی که بسیار بیشتر یا کمتر از دو استاندارد انحراف از آمار عادی به وقوع می پیوند،غیرعادی فرض می شود.به عنوان مثال اگر کاربری به جای یک یا دو بار ورود و خروج عادی به سیستم در طول روز،بیست بار این کار را انجام دهد، و یارانه ای که در ساعت ۲:۰۰ بعد از نیمه شب مورد استفاده قرار گرفته در حالی که قرار نبوده کامپیوتر فوق پس از ساعت اداری روشن باشد هر یک از این موارد می تواند به عنوان یک رفتار غیرعادی در نظر گرفته شود.به منظور پیاده سازی سیستم های تشخیص نفوذ سیستم های متعددی طراحی و ساخته شده اند .در حوزه امنیت کامپیوتر،سیستم های تشخیص نفوذ هشداردهنده را ایفا می کنند و هر زمان که امنیت شبکه در معرض خطر قرار می گیرد،آن را اعلام می کنند.

از طرف دیگر شبکه های عصبی به عنوان یکی از تکنیک های داده کاوی کاربرد زیادی در یافتن الگوها در سیستم تشخیص نفوذ دارند.شبکه های عصبی به شبیه سازی رفتار بیولوژیکی نرون ها برای تامین یک ابزار موثر در حل مسائل طبقه بندی می پردازند.شبکه های عصبی می توانند به ایجاد دانش با الگوهای ورودی دیده نشده بپردازند،همچنین دارای یک سرعت نسبی در محاسبات و قدرت بالای تطابق با محیط می باشند.به همین دلیل اگر بر روی بخشی از شبکه صدمه ای وارد شود ، تاثیر کمی بر روی ظرفیت محاسباتی شبکه می گذارد از این تکنیک در سیستم های تشخیص نفوذ استفاده می شود[4].

تشخیص نفوذ به کمک داده کاوی:

ایجاد بستر مناسب:

یک بستر مناسب برای انجام یک فرایند تشخیص نفوذ به کمک داده کاوی به ترتیب نیازمند موارد زیر است:

- پایگاه داده:چرا که ما نیازمند محلی، با ساختار مشخص و استاندارد برای ذخیره داده ها هستیم داده های این پایگاه داده بایستی به صورت مرتب بروزرسانی شود و بایستی دارای مکانیزم پاسخگویی سریعی برای بازجست ها باشد .بدین منظور بایستی از سیستم های مدیریت پایگاه داده معروف استفاده گردد.
- فضای کاری :برای بکار بردن یک سیستم تشخیص نفوذ، نیازمند داده و فضای کاری متناسب برای انجام داده کاوی هستیم همچنین داده ها بایستی مشغول محاسبات و ذخیره سازی متاداده هابه همان سرعت کپی کردن داده های عادی

[5] Misuse Detection
[6] Anomaly Data
[7] Labeled Data

باشد .فضای کاری بایستی دارای مجموعه داده های نمونه متنوع برای انجام آزمایشات دادهکاوی باشد .همچنین ابزارهای ذخیره سازی برای استفاده های خاص بسیار موردنیاز هستند.

- قابلیت محاسبه :انجام فرایندهای داده کاوی توسط ابزارهای داده کاوی به واحد پردازنده مرکزی و حافظه اصلی و جانبی زیادی احتیاج دارد پس افزایش توان محاسباتی و سرعت واحد پردازنده مرکزی و ظرفیت حافظه طبیعی است . بررسی ها نشان می دهد که انجام تشخیص نفوذ با استفاده از داده کاوی به چهار برابر منابع بیشتر نسبت به انجام تشخیص نفوذ بدون استفاده از داده کاوی، نیاز دارد.
- نرم افزار :علاوه بر در اختیار داشتن نرم افزار های پایه مانند سیستم عامل، پایگاه داده استاندارد با قابلیت ها و کیفیت بالا، نیازمند در اختیار داشتن ابزارهای داده کاوی به همراه حق مالکیت آنها است .ابزارهای بسیاری برای انجام فرایندهای داده کاوی ایجاد شده است که می توان به Gritbot ،. eka ، Clementineشاره کرد.

لازم است بدانید صرف داشتن ابزارهای داده کاوی برای انجام فرایند داده کاوی کافی نیست و نیاز به تخصص و شخصی که بتواند از ابزارهای به صورت موثر استفاده کند و تجربه کاری مرتبط داشته باشد، می باشد.

تکنیک های داده کاوی:

برای ساختن مدلهای تشخیص نفوذ از تکنیک های داده کاوی استفاده می شود. هدف از این روش این است که الگوهای سازگار و مفیدی از ویژگیهای سیستم کشف شود.به طوری که بتوان از آنها رفتار کاربران و برنامه را توصیف نمود این مجموعه از ویژگیها می توانند توسط روش های استقرایی پردازش شوندتا دسته بندی کننده هایی(موتورهای تشخیص) را شکل دهند که قادرند سناریوهای سوء استفاده در رفتارهای غیرعادی را شناسایی کنند.داده کاوی به فرآیند استخراج(خودکار) الگوها از دسته های بزرگی از داده ها رجوع می کند. الگوریتم های متعددی از قبیل دسته بندی،تحلیل ارتباط و تحلیل توالی برای اهداف داده کاوی موجود هستند.

روش های آماری :

که فنون متداول آن شامل:استنباط بیزی، رگرسیون لوژستیکی ، تحلیل ANOVA و مدل های غیرخطی.

تحلیل خوشه ای:

که یک فن عمومی بوده و دارای الگوریتم های تقسیم پذیری،متراکم سازی ،خوشه بندی افزاری و خوشه بندی نموی می باشد.

قواعد و درخت های تصمیم گیری:

مجموعه ای از روش های یادگیری استقرایی هستند که عموما در هوش مصنوعی طرح و توسعه یافته اند.فنون ساده شامل روش CLS ، الگوریتم C4.5 الگوریتم های حذفی متناظر می باشند.

قواعد پیوندی[8]:

یک مجموعه نسبتا جدید از روش ها را ارائه می کند و شامل الگوریتم هایی مانند تحلیل سبد خرید ،الگوریتم برهان و الگوی فروش دوره ای WWW می باشند.

شبکه عصبی مصنوعی :

که در آن تاکید بر روی ادراک های چندلایه ای با یادگیری انتشار معکوس و شبکه های کوهنن می باشد.

[8] Association Rules

الگوریتم های ژنتیک:

که به عنوان متدلوژی برای حل مسائل بهینه سازی سخت بسیار سودمند می باشد.

سیستم های استنباط فازی:که بر اساس نظریه مجموعه های فازی و منطق فازی می باشند.مدل سازی فازی و تصمیم گیری فازی گام های معمول در فرآیندهای داده کاوی می باشند.

روش های مصنوعی n[9] بعدی:

که معمولا در نوشته ها به عنوان یک متدولوژی داده کاوی استاندارد از آن رد می شوند،اگرچه ممکن است اطلاعات مفیدی را با استفاده از این ابزارها و فنون به دست آورد.فنون تجسمی متداول داده کاوی عبارتند از: فنون هندسی،مبتنی بر نشانه ،جهت پیکسلی و سلسله مراتبی.

جدول ۱: مقایسه الگوریتم ها از سه منظر

نام الگوریتم	دقت	نرخ هشدارهای کاذب	نرخ محاسباتی
الگوریتم Bayesian در تشخیص نفوذ[1]	نرخ دقت بالا درتشخیص نفوذ	کاهش نرخ هشدار منفی	هزینه محاسباتی نسبتاً کمتر
الگوریتم APRIORI و قوانین انجمنی [2]	با قوانین انجمنی نرخ تشخیص نفوذ تا حد زیادی بالامی رود.	کاهش نرخ هشدار منفی	هزینه محاسباتی بهتر
الگوریتم قوانین وابستگی و الگوریتم (Rough Set)[3]	تشخیص نفوذ با استفاده از قوانین وابستگی می تواند بهبود یابد.	کاهش نرخ هشدار منفی	هزینه محاسباتی بهتر
الگوریتم classification و ارائه الگوریتم ترکیبی دیگری به نام ۲class classification [4]	سرعت تشخیص نفوذ بالاتری نسبت به دسته بندی معمولی دارد.	کاهش نرخ هشدار منفی و مثبت	هزینه محاسباتی نسبتاً بالایی نسبت به مدل اولیه خود دارد.
الگوریتم ژنتیک [5]	فرآیند تشخیص نفوذ و نرخ تشخیص بالاتر است.	کاهش نرخ هشدار مثبت	بهبود شاخص بازدهی محاسباتی
الگوریتم درخت افزایشی و الگوریتم Rough Set [۶]	دقت نسبتاً کمتری به روش های مشابه دیگر به خاطر افزایش	کاهش نرخ هشدار منفی	هزینه محاسباتی بالا

شکل۱- جدول مقایسه الگوریتم های تشخیص نفوذ مبتنی بر داده کاوی

تست نفوذ:

سیستم های تشخیص نفوذ[10] به عنوان یکی از عناصر اصلی زیرساخت های امنیت در بسیاری از سازمان ها می باشد.این سیستم ها،مدل ها و الگوهای سخت افزاری و نرم افزاری می باشند که به خودکار کردن فرآیندهایی می پردازد که این فرآیندها به بررسی وقایع اتفاق افتاده در شبکه یا سیستم های کامپیوتری می پردازد.سیستم های تشخیص نفوذ به بررسی و تحلیل این وقایع رخ داده شده برای حل مسائل امنیت سیستم ها و شبکه های کامپیوتری می پردازند [5] اگر چه بسیاری از این اخطارها صحیح نمی باشند و اصطلاحاً اخطارهای غلط می باشند،شواهدی وجود ندارد که نشان دهدآیا این اخطارها صحیح هستند یا غیرصحیح که این موضوع نیاز به بررسی زیادی دارد.تکنیک های متعددی وجود دارد که به شناسایی اخطارهای صحیح و ناصحیح می پردازد و بدین ترتیب کارآیی و عملکرد سیستم های تشخیص نفوذ بالاتر می رود[5].

سیستم های تشخیص نفوذ به تلاش برای شناسایی فعالیتهای کاربر به دو صورت نرمال و آنومالی می پردازد و این کار توسط مقایسه تراکنش های اتصال به شبکه بر مبنای الگوهای شناخته شده نفوذ توسط متخصصان و خبرگان بدست آمده و گراحی

[9] Visualization
[10] Intrusion detection systems

شده است.روش های سنتی نمی توانند به صورت کارا به کشف الگوهای ناشناخته نفوذ بپردازند زیرا نیروی انسانی در حین انجام تحلیل ، تشخیص نفوذ با شبکه هایی از سیستم های کامپیوتری مواجه می شود که سرعت و پیچیدگی بالایی دارند،لذا در این خصوص از تکنولوژی های تصمیم هوشمند بر مبنای داده کاوی استفاده می شود ، تا الگوهای کارآمد و موثری در تشخیص نفوذ شناسایی شود [6].

یک تست نفوذ[11] یا یک پروسه مجاز،برنامه ریزی شده و سیستماتیک برای به کارگیری آسیب پذیری ها جهت نفوذ به سرور ،شبکه و یا منابع برنامه های کاربردی است. در واقع تست نفوذ روشی برای ارزیابی امنیتی یک سیستم یا شبکه کامپیوتری است که از طریق شبیه سازی حمله یک هکر یا نفوذگر خرابکار صورت می گیرد.پروسه تست نفوذ یک تحلیل فعال از سیستم برای یافتن هر حفره،آسیب پذیری و نقص فنی است که بالقوه یک ضعف امنیتی سیستم محسوب می شود.این تحلیل در مقام یک هکر بالقوه انجام می شود و دی آن می توان از آسیب پذیری امنیتی فعال برای اجرای حملات استفاده کرد همه مشکلات امنیتی باید همراه با ارزیابی میزان اهمیت آنها و همچنین پیشنهادهایی برای کاهش اثر خطرات و یا راه حل های فنی به صاحب سیستم ارائه شوند.تست نفوذ می تواند با استفاده از منابع داخلی همچون سیستم امنیتی میزبان و یا منابع خارجی همچون سیستم امنیتی میزبان ویا منابع خارجی همچون سیستم امنیتی میزبان و یا منابع خارجی همچون اتصالات شرکت به اینترنت هدایت شود.در این تست معمولا از یک سری ابزارهای اتوماتیک و یا دستی برای آزمودن منابع سیستم استفاده می شود.البته انجام تست نفوذ بر روی سیستم های فعال ،خطر از هم گسستن آنها را در پی دارد زیرا اجرا کردن حملات فعال بر روی سیستم ممکن است منجر به از کارافتادگی ،بروز برخی رفتارهای غیرقابل پیش بینی و بی ثباتی سیستم شود[7].

انواع واکنش سیستم های تشخیص نفوذ:

در واکنش به گزارش هایی که توسط سیستم های تشخیص نفوذ در سطح شبکه می شود ، دو نوع عکس العمل وجود دارد که به ترتیب عکس العمل های فعال[12] و غیرفعال[13] می باشد. در ادامه به بررسی این دونوع عکس العمل ها در برخورد به گزارش های سیستم های تشخیص نفوذ تحت شبکه خواهیم پرداخت.

واکنش غیر فعال[14]:

واکنش غیرفعال معمولترین واکنشی است که به بیشتر نفوذها در شبکه انجام می شود.در واقع واکنش های غیرفعال ساده ترین و راحت ترین واکنش در برخورد با نفوذ ها برای پیاده سازی و توسعه هستند .استراتژی های واکنش های غیرفعال شامل موارد زیر است[7]

لاگ برداری[15] :

لاگ برداری شامل ضبط کلیه رویدادهای شبکه است که اتفاق می افتند و همچنین چگونگی رخ دادن آنها را نیز نمایش می دهد.لاگ برداری بایستی به شکلی اطلاعات را در اختیار مدیران قرار دهند که آنها بتوانند از طریق این داده ها ذات حمله

[11] Penetration Test
[12] Active
[13] Passive
[14] Passive Response [۱۷] Shunning
[15] Logging

و چگونگی به وقوع پیوستن آن را ارزیابی کنند. این اطلاعات بعدها می توانند برای طراحی راهکارها برای مقابله با تهدیدات مورد استفاده قرار بگیرند.

آگاه سازی[۱۶] :

آگاه سازی در واقع ارتباطی است که از طریق آن اطلاعات مربوط به رویداد اتفاق افتاده به شخص مسئول آن ارسال می شود. این شامل هرگونه اطلاعاتی است که می تواند به مدیر سیستم کمک کند تا در مورد حادثه درک بهتری داشته باشد،اگر سیستم تشخیص نفوذ بصورت تمام وقت مشغول به فعالیت است ،پیامها بر روی کنسول مدیریتی نمایش داده خواهد شد تا زمانیکه مسئول سیستم آنها را مشاهده و نظارت کند.

اجتناب کردن[۱۷] :

اجتناب کردن یا چشم پوشی از حمله یک واکنش معمول است . برای مثال سیستم تشخیص نفوذ شما از بروز حمله از نوع حملات به وب سرور IIS به سیستمی گزارش می دهد که دارای وب سرور آپاچی می باشد،در این حالت نیازی به انجام هیچگونه عمل متقابلی نخواهد بود زیرا حمله به طور یقین ناکارآمد خواهد بود.خوب در چنین شرایطی که مطمئن هستیم حملاتی که بر روی IIS انجام می شوند بر روی آپاچی موثر نخواهند بود،آیا نیازی به صرف وقت و هزینه برای مقابله با آن وجود دارد؟در یک شبکه بزرگ بسیاری از این نوع حملات ممکن است بصورت همزمان بوجود بیایند،نکته در اینجاست که اگر موفق بودن یا ناموفق بودن یک حمله در شبکه برای شما اهمیتی ندارد،پس چرا برای کشف و شناسایی و اطلاع رسانی آن انرژی صرف کنیم؟در اینگونه موارد از این نوع حملات چشم پوشی کرده و به کارهای مهمتری در شبکه می پردازیم.

واکنش فعال[۱۸]:

واکنش فعال بدین معناست که در مقابل حمله یا تهدید موجود عکس العمل نشان بدهیم.هدف واکنش فعال انجام دادن سریعترین عمل ممکن در جهت کاهش تاثیرات احتمال رویدادی است که اتفاق افتاده است.این نوع از واکنش ها برای اینکه بتوانند موثر باشند نیازمند طراحی اولیه برای شیوه برخورد با رویدادها،خط مشی های واضح و صریح تبیین شده و همچنین هوشیاری خاصی می باشند[8].

خصیصه های مناسب در تشخیص نفوذ در شبکه های کامپیوتری:

رکوردهای داده ای دارای تعداد زیادی خصیصه هستند .هنگامی که به منظور تشخیص نفوذ در شبکه های کامپیوتری از داده کاوی استفاده می کنیم بایستی از داده های سطح TCPDUMP استفاده کنیم .

از دسته Sniffer است و یا به عبارت ساده تر عملاً یک تحلیل گر ترافیک شبکه است نرم افزار قدیمی و مشهور TCPDUMP تحت سیستم عامل خانواده ی Unix می باشد .عملاً یک تحلیلگر ترافیک شبکه است یک تحلیل گر ترافیک

[16] Notification

[۱۸] Active Response

شبکه که عموماً با نام Sniffer از آن یاد می گردد، وظیفه ی بررسی بسته های رد و بدل شده بر روی شبکه را بر عهده دارد که با استفاده از یک Sniffer با تعیین یک رابط شبکه ی خاص، می توان ، با پایش و تحلیل بسته های اطلاعاتی رد و بدل شده بر روی شبکه ای که رابط شبکه ی مورد نظر به آن متصل است پرداخت به عبارت دیگر یک Sniffer را می توان به یک سیستم پایش تشبیه کرد که تمامی اطلاعات منتقل شده بر روی یک بستر فیزیکی را بررسی و ذخیره می کند و یا از داده های سطح هشدار استفاده کرد. در هر دو نوع داده فیلدهایی برای آدرس IP مبدأ و مقصد، شماره پورت مبدأ و مقصد، تاریخ، زمان، پروتکل انتقال (TCP ,UDP ,ICMP ,ETC) و زمان آغاز و پایان ترافیک خواهیم یافت .این خصیصه های پایه، توصیف مناسبی از یک ارتباط خاص یا یک هشدار را ارائه می دهند اما اغلب برای شناسائی ارتباط های غیرمتعارف و مشکوک کافی نیستند.

نتیجه گیری:

سیستم های تشخیص نفوذ سیستمی است که بایستی امنیت و حداقل هشدار یا آلارم صحیحی از خود نشان دهد.امنیت مسئله بسیار مهمی است که بایستی با احتمال بالاتری در سیستم تشخیص نفوذ ، طراحی گردد.گاهی سخت افزار برای محاسبات مد نظر شخص یا سازمان نیست و می توان سخت افزار مورد نیاز برای محاسبات را تهیه کرد لذا روشها و الگوریتم هایی در جدول شماره فلان معرفی شده اند که می توان از آنها استفاده کرد.به منظور رسیدن به درجه ی بالای اعتماد معمولا سیاست های امنیتی در نظر گرفته می شود.این سیاستها عملکرد بخش های مختلف سیستم را کنترل کرده و نیازمندی های لازم جهت اعمال نظارت را مشخص می کنند.

سیستم تشخیص نفوذ شبکه های اجتماعی اشکالاتی مانند Single Point Failed را ندارد در سیستم های دیگر رفع شده است و همچنین دامنه تحت پوشش و بکارگیری سیستم گسترش یافته و در عین حال همچنان تصمیم گیری محلی باقی مانده است که از مزایای سیستم تشخیص نفوذ شبکه های اجتماعی به شمار می آید هدف از طراحی سیستم تشخیص نفوذ شبکه های اجتماعی، ارائه معماری برای اشتراک دانش بین سیستم های تشخیص نفوذ می باشد.این سیستم می تواند به عنوان مکمل سیستم های تشخیص نفوذ فعلی با هر نوع از معماری استفاده گردد و امکان اشتراک دانش بین سیستمهایی از انواع مختلف را فراهم نماید.با گسترش دامنه تشخیص یک سیستم تشخیص نفوذ،باعث بهبود کارآیی آن در شناخت نفوذها می گردد .بدیهی است هر چه تنوع دانشهای به اشتراک گذاشته شده بیشتر باشد ، نتایج بهتری نیز حاصل خواهد گردید همچنین برای دستیابی به زمان منطقی در همگرایی بایستی با افزایش تعداد نودها،تعداد دانش قابل مبادله افزایش و یا زمان توزیع کاهش یابد.

مراجع:

[1] Ngai, Eric WT, Li Xiu, and D. C. K. Chau. "Application of data mining techniques in customer relationship management: A literature review and classification." Expert Systems with Applications 3662 (2009): 2592-2602.

[2] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez,David Isacoff, Eugene Spafford, and Diego Zamboni. "An architecture for intrusion detection using autonomous agents",
Proceedings of the Fourteenth Annua Computer Security Applications Conference, pp 13–24, IEEE Computer Society

[3] Panda, Mrutyunjaya, Ajith Abraham, and Manas Ranjan Patra. "A Hybrid Intelligent Approach for Network Intrusion Detection." Procedia Engineering 30 (2012): 1-9.

[4] Srinivasu, P., and P. S. Avadhani. "Genetic Algorithm based Weight Extraction Algorithm for Artificial Neural Network Classifier in Intrusion Detection."Procedia Engineering 38 (2012): 144-153.

[5] Altwaijry, H. and Algarny, S., (2012), Bayesian based intrusion detection system, Journal of King Saud University– Computer and Information Sciences, Vol. 24, pp. 1-6.

[6] Altwaijry, Hesham. "Bayesian based intrusion detection system." IAENG Transactions on Engineering Technologies. Springer Netherlands, 2013. 29-44.

[7] Lee, David, et al. "Passive testing and applications to network management."Network Protocols, 1997. Proceedings., 1997
International Conference on. IEEE, 1997.

[8] Wang, Xinyuan, et al. "Sleepy watermark tracing: An active network-based intrusion response framework." Proc. of the 16th International Information Security Conference. 2001.

[9] Hanguang, L. and Yu, N., (2012), Intrusion Detection Technology Research Based on Apriori Algorithm, 2012 International Conference on Applied Physics and Industrial Engineering, hysics Procedia, Vol. 24, pp. 1615-1620.

[10] Said, Karim A. PicoRF: A PC-based SDR Platform using a High Performance PCIe Plug-in Card Extension. Diss. Virginia Polytechnic Institute and State University, 2012.

[11] Tao Peng, Christopher Leckie, "Information sharing for distributed intrusion detection systems", 2007.

[12] Karen Scarfone, Peter Mell, "Guide to Intrusion Detection and Prevention Systems", 2007. [11] Li, Lu, et al. "The application of genetic algorithm to intrusion detection in MP2P network." Advances in Swarm Intelligence (2012): 390-397.

[13] Denatious, D.K, John, " A Survey on data mining techniques to enhance intrusion detection " Computer Communication and Informatics (ICCCI), 2012 International Conference on DOI: 10.1109/ICCCI.2012.6158822

[14] Yusufovna, S.F. ''Integrating Intrusion Detection System and Data Mining '' , Ubiquitous Multimedia Computing, 2008. UMC '08. International Symposium on
DOI: 10.1109/UMC.2008.59

[15] Dartigue, C. ; Hyun Ik Jang ; Zeng, Wenjun,'' A New Data-Mining Based Approach for Network Intrusion Detection '' , Communication Networks and Services

Research Conference, 2009. CNSR '09. Seventh Annual
DOI: 10.1109/CNSR.2009.64
[16] Gudadhe, M. ; Prasad, P. ; Wankhade, K.'' A new data mining based network Intrusion Detection model '' Computer and Communication Technology (ICCCT), 2010 International Conference onDOI: 10.1109/ICCCT.2010.5640375

[17] Ektefa, M. ; Memar, S. ; Sidi, F. ; Affendey, L.S''Intrusion detection using data mining techniques '' Information Retrieval & Knowledge Management, (CAMP), 2010 International Conference onDOI: 10.1109/INFRKM.2010.5466919

[18] علیرضا بینا،سعید آیت،کاوش قوانین فازی در سیستمهای تشخیص نفوذ با استفاده از اتوماتای یادگیری سلولی،چهارمین کنفرانس داده کاوی تهران ،۱۳۸۹