
بسم الله الرحمن الرحيم
بسم الله الرحمن الرحيم
بسم الله الرحمن الرحيم

معاونت پژوهش و فن آوری

به نام خدا

شورا اخلاق پژوهش

با یاری از خداوند سبحان و اعتقاد به این که عالم محضر خداست و همواره ناظر بر اعمال انسان و به منظور پاس داشت مقام بلند دانش و پژوهش و نظر به اهمیت جایگاه دانشگاه در اعتلای فرهنگ و تمدن بشری، ما دانشجویان و اعضاء هیات علمی واحدهای دانشگاه آزاد اسلامی متعهد می گردیم اصول زیر را در انجام فعالیت های پژوهشی مد نظر قرار داده و از آن تخطی نکنیم:

۱- اصل حقیقت جویی: تلاش در راستای پی جویی حقیقت و وفاداری به آن و دوری از هرگونه پنهان سازی حقیقت.

۲- اصل رعایت حقوق: التزام به رعایت کامل حقوق پژوهشگران و پژوهیدگان (انسان، حیوان و نبات) و سایر صاحبان حق.

۳- اصل مالکیت مادی و معنوی: تعهد به رعایت کامل حقوق مادی و معنوی دانشگاه و کلیه همکاران پژوهش.

۴- اصل منافع ملی: تعهد به رعایت مصالح ملی و در نظر داشتن پیشبرد و توسعه کشور در کلیه مراحل پژوهش.

۵- اصل رعایت انصاف و امانت: تعهد به اجتناب از هرگونه جانب داری غیر علمی و محافظت از اموال، تجهیزات و منابع در اختیار.

۶- اصل رازداری: تعهد به صیانت از اسرار و اطلاعات محرمانه افراد، سازمان ها و کشور و کلیه افراد و نهادهای مرتبط با تحقیق.

۷- اصل احترام: تعهد به رعایت حریم ها و حرمت ها در انجام تحقیقات و رعایت جانب نقد و خودداری از هرگونه حرمت شکنی.

۸- اصل ترویج: تعهد به رواج دانش و اشاعه نتایج تحقیقات و انتقال آن به همکاران علمی و دانشجویان به غیر از مواردی که منع قانونی دارد.

۹- اصل برائت: التزام به برائت جویی از هرگونه رفتار غیر حرفه ای و اعلام موضع نسبت به کسانی که حوزه علم و پژوهش را به شائبه های غیر علمی می آلایند.

دانشگاه آزاد اسلامی

واحد علوم تحقیقات

تعهدنامه اصالت رساله یا پایان نامه

اینجانب **مریم بهنام** دانش آموخته مقطع کارشناسی ارشد ناپیوسته در رشته **نرم افزار کامپیوتر** که در تاریخ ۹۲/۸/۲۸ از پایان نامه / رساله خود تحت عنوان" استفاده ازتکنیکهای داده کاوی درسیستمهای تشخیص نفوذ "با کسب نمره **۱۹** ودرجه **عالی** دفاع نموده ام بدینوسیله متعهدمی شوم:

۱) این پایان نامه / رساله حاصل تحقیق وپژوهش انجام شده توسط اینجانب بوده ودر مواردي که از دستاوردهاي علمی وپژوهشی دیگران اعم از(پایان نامه، کتاب، مقاله و ...)استفاده نموده ام، مطابق ضوابط ورویه موجود، نام منبع مورد استفاده وسایر مشخصات آن را درفهرست مربوطه ذکر و درج کرده ام.

۲) این پایان نامه / رساله قبلا "براي دریافت هیچ مدرك تحصیلی(هم سطح، پائین تریا بالاتر) در سایر دانشگاه ها ومؤسسات آموزش عالی ارائه نشده است.

۳) چنانچه بعد از فراغت از تحصیل، قصد استفاده و هرگونه بهره برداري اعم از چاپ کتاب، ثبت اختراع و ... از این پایان نامه داشته باشم، از حوزه معاونت پژوهشی واحد مجوزهاي مربوطه را اخذ نمایم.

٤) چنانچه در هر مقطع زمانی خلاف موارد فوق ثابت شود، عواقب ناشی ازآن را می پذیرم و واحد دانشگاهی مجاز است با اینجانب مطابق ضوابط ومقررات رفتار نموده و درصورت ابطال مدرك تحصیلی ام هیچ گونه ادعایی نخواهم داشت.

نام ونام خانوادگی:**مریم بهنام**
تاریخ و امضاء:**۹۲/۸/۲۸**

دانشگاه آزاد اسلامي

واحد علوم و تحقيقات شاهرود

دانشكده فني مهندسي،گروه كامپيوتر

پايان نامه براي دريافت درجه كارشناسي ارشد در رشته مهندسي كامپيوتر (M.Sc)

گرايش: نرم افزار

عنوان:

استفاده از تکنیک های داده کاوی در سیستم های تشخیص نفوذ

استاد راهنما:

دكترسيد هاشم طبسي

استاد مشاور:

دكتر محمود معلم

نگارش:

مريم بهنام

پاييز ۱۳۹۲

سپاسگزاری

خداوند متعال را شاکرم که این توفیق را نصیب من نمود تا بتوانم این پایان نامه را به پایان برسانم .
برخود لازم مي‌دانم از اساتید ارجمند جناب آقاي دکتر طبسی به عنوان استاد راهنما و جناب آقای دکترمعلم به عنوان استاد مشاور که با راهنمایی های خود باعث فراهم آوردن فرصتی جهت تحقیق در این زمینه شدند و باصبر و حوصله بسیار مرا در این مسیرهدایت فرمودند ، کمال تشکر را داشته باشم .
از استاد ارجمند جناب آقای دکتر پور قلی که زحمت مطالعه و داوری این پایان نامه را برعهده داشته اند، تشکر و قدردانی می نمایم .
همچنین از خانواده عزیزم که همیشه حامی و مشوق من بوده اند و در راه پیشرفتم از هیچ تلاشی فرور گذار نکرده اند سپاسگزاری می نمایم.
در نهایت از دوستان خوبم که همیشه یارو یاورم بوده اند سپاسگزارم .

مریم بهنام – آبان ۱۳۹۲

تقدیم به پدر و مادر عزیزم
که زحماتشان جبران نشدنی است

فهرست مطالب

عنوان — شماره صفحه

فصل پنجم : تجزیه و تحلیل داده ها و نتیجه گیری

فهرست شکل ها

عنوان | شماره صفحه

فهرست جداول

فهرست نمودارها

عنوان | شماره صفحه

چکیده فارسی:

فرایندتشخیص نفوذنظارت برروییدادهایی است که درسیستم هاي کامپیوتري ویاشبکه اتفاق می افتدو آنها رابراي شناسایی نفوذتجزیه وتحلیل می کند .چگونگی تشخیص حملات شبکه بخش مهمی درسیستم هاي تشخیص نفوذاست.

دراین پایان نامه سیرتکامل قوانین براساس برنامه نویسی ژنتیک براي تشخیص نفوذدرشبکه معرفی شده است که الگوهاي حملات شناخته شده راتشخیص می دهدو با ارتقا روش جدید به نام برنامه نوبسی بیان ژن(Gene Expression Programming(GEP ازژنوم خطی به همراه عملگرهاي ژنتیکی مانند جهش، ترکیب، وارونسازي وجابجایی برای این کاراستفاده می کند.در نهایت با شاخص های دقت طبقه بندي،نرخ مثبت صحیح (TPR)ونرخ مثبت کاذب (FPR)بازده ی سیستم تشخیص نفوذپیشنهادی نسبت به سیستم های مرسوم قبلی نشان داده شده است. نتایج نشان می دهدتکنیک هاي برنامه نویسی ژنتیکی استفاده شده براي تشخیص نفوذ از روشهای مشابه خود که براساس الگوهاي یادگیري ماشین هستنداز دقت بالاتري برخورداراست. ازمجموعه داده به نام KDDCUP99 که انواع حملات شبکه را درخودجاي داده است استفاده می نماییم .

کلمات کلیدی
سیستم تشخیص نفوذ، یادگیری ماشین، برنامه نویسی ژنتیک، برنامه نویسی بیان ژن

فصل اول

۱-۱- مقدمه

همگام با رشد شبکه های کامپیوتری حملات و نفوذ ها به این شبکه گسترش یافته و به روشهای متعددی انجام می شود . نفوذ مجموعه اقدامات غیر قانونی است که صحت ، محرمانگی و یا دسترسی به یک منبع را به خطر می اندازد . نفوذ گران را می توان به دو دسته نفوذگران داخلی و نفوذگران خارجی دسته بندی کرد.
نفوذگران خارجی کسانی هستند که اجازه استفاده از سیستم را ندارند اما سعی می کنند سیستم را مورد دسترسی قرار دهند و نفوذ گران داخلی کسانی هستند که به سیستم اختیارات محدودی دارند اما سعی می کنند به منابعی که اجازه دسترسی به آن را ندارند ، دسترسی پیدا کنند .
به منظور مقابله با نفوذ گران به شبکه ها و سیستم های کامپیوتری ، روشهای متعددی تعیین شده است که روشهای تشخیص نفوذ نامیده میشوند. هدف از تشخیص نفوذ این است که استفاده غیر مجاز ، سوء استفاده و آسیب رساندن به سیستم ها و شبکه های کامپیوتری توسط هر دو دسته کاربران داخلی و حمله کنندگان خارجی شناسایی شود.
بطور کلی روشهای تشخیص نفوذ به دو دسته اصلی تشخیص سوء استفاده و تشخیص رفتار غیر عادی تقسیم میشوند. در روش تشخیص سوء استفاده از الگوهای نفوذ شناخته شده برای شناسایی نفوذ ها استفاده می شود. درحالی که روشهای تشخیص رفتار غیر عادی ، رفتار عادی کاربران ملاک عمل قرار داده میشود و در نتیجه هرگونه مغایر با آن به عنوان تلاش جهت نفوذ به سیستم شناسائی می گردد.
به منظور پیاده سازی روشهای تشخیص نفوذ ، سیستم های متعددی طراحی و ساخته شده اند. در حوزه امنیت کامپیوتر ، سیستمهای تشخیص نفوذ نقش هشدار دهنده را ایفا می کنند و هر زمان که امنیت شبکه در معرض خطر قرارمی گیرد ، آن را اعلام می کنند. نهاد دیگری که مسئول امنیت سایت نامیده می شود ، می تواند به این هشدار ها پاسخ داده و راهکارهای مناسب را اجرا کند.
سیستم های تشخیص نفوذ اولیه با تحلیل فایل رخدادها که توسط سیستم عامل و برنامه های کاربردی ایجاد میشوند ، کار می کردند . اما به مرور که شبکه ها پیچیده شدند به داده های کافی برای شناسایی قاطعانه یک حمله دسترسی نداشتند. بنابراین با توجه به روشهای تشخیص نفوذ پیچیده تر مبتنی بر تحلیل داده های شبکه یا میزبان معطوف شد.
نفوذگرها معمولا از عیوب سخت افزاری ، شکستن کلمات رمز ، استراق سمع ترافیک شبکه و نقاط ضعف طراحی برای نفوذ به سیستم و شبکه های کامپیوتری استفاده می کنند.
اغلب لازم است با کشف هر حمله جدید تشخیص نفوذ بروز رسانی شود . سازندگان این سیستم ابتدا سناریوهای حمله و نقاط ضعف سیستم را تجزیه تحلیل و طبقه بندی می کنند . به دلیل ماهیت دستی و غیر الگوریتمی فرآیند توسعه در سیستمهای تشخیص نفوذ ، اعمال تغییرات در آن کند و پر هزینه است .

۱-۲- مروری بر پیشینه تحقیق

(عظیمیان و دیگران ۱۳۸۹) از تکنیکهای داده کاوی در زمینه یادگیری ماشین و از الگوریتمهای ماشین بردار پشتیبان (SVM)[۱] , الگوریتم درخت تصمیم(C4.5) استفاده کردند واز روش تشخیص سوء استفاده، به منظور تشخیص نفوذ در شبکه های کامپیوتری مقایسه و ارزیابی شده است. نتایج حاصل از آزمایشات از بین معیار های ارزیابی آنها نشان می دهد که در حالت میانگین ، C4.5 در معیارهای Detection rate و Precision بهتر عمل نموده است ،اما در معیاری False alarm rate، SVM عملکرد بهتری داشته است. همچنین با توجه به معیارAccuracy عملکرد C4.5 کمی بهتر از SVM می باشد.

(معدني پور، ابوالحسني و شيرازي۱۳۸۹) روشی از مفاهيم داده كاوي و تحليل شبكه هاي اجتماعي پيشنهاد كرده اند. روشهاي موجود براي انتخاب ويژگي ذكر شدندكه هركدام مزايا و معايبي دارند .تنها برخي از آنها قادر به رتبه بندي ويژگيها از نظر اهميت هستند و هيچ يك قادر به بيان نحوه ارتباط ويژگي های تشخيص نفوذ نمي باشند .با توجه به نتايج نشان داده شده كه روش Rough-PSO (Particle Swarm optimization)مي تواند مجموعه بهينه مرتبط با هرنوع حمله را بيان كند كه هزينه اجراي آن نمايي است.

(علی زاده ، مقدادی۲۰۱۲) به مطالعه ی انواع حملات و سیستم های تشخیص ناهنجاری و سیستم های تشخیص سوء استفاده تاکید دارند وبه معرفی انواع تکنیک های مورد استفاده در سیستم های تشخیص نفوذ می پردازند.برخی از این تکنیک ها مبتنی بر محاسبات هستند نظیر منطق فازی و شبکه های بیزین ،برخی مبتنی بر هوش مصنوعی هستند نظیر سیستم های خبره و شبکه های عصبی و برخی دیگر مفاهیم بیولوژیکی نظیر سیستم های ژنتیکی و ایمنی می باشند.

(سلطانی زاده ، برادران شکوهی وزارع۱۳۹۰) الگوریتم جدیدی جهت دسته بندی داده ها بر مبنای روش ایمنی مصنوعی و تلفیق آن با روش تپه نوردی(Hill Climbing) به منظور پیاده سازی سیستم تشخیص نفوذ ارائه نمودند .داده های مورد تست و آزمون این الگوریتم NSL-KDD می باشد که بروی ۷۴۵۳ داده TCP در مجموعه داده تست گردیده است .

(ابطحي ، ميبدی۱۳۸۷) يك مدل سلسله مراتبي از عامل هاي مبتني برآتوماتاي يادگير براي تشخيص نفوذهاي از نوع انكار سرويس مطرح نمودند .در مدل پيشنهادي هر عامل داراي يك آتوماتاي يادگير است كه پارامترهاي مدل را نگهداري كرده و آنها را با توجه به بازخوردهايي كه از محيط دريافت مي كنند به روز مي رسانند .در مدل ارائه شده مسئله تشخيص نفوذ به صورت يك مسئله دسته بندي دوكلاسه مطرح مي گردد. براي آموزش و آزمايش اين مدل، از مجموعه داده های KDD99 استفاده شده كه يك مجموعه داده استاندارد برای كاربردهاي امنيتي مي باشد .

(زندي ، فتحي و شرايعي۱۳۹۰) با تعريف نفوذ، و داده كاوي به بررسي كاربردهای داده كاوي در تشخيص نفوذ پرداخته اند. سيستم هاي تشخيص نفوذي كه بر اساس داده كاوي طراحي شده اند در شبكه هاي محلي داراي عملكرد بسيارخوبي هستند.در سيستم هاي تجاري ازالگوي و امضاي حملات شناخته شده استفاده مي گردد .به اينگونه امضاها، امضاهاي ايستا گويند، اين بدان معناست كه امضا والگوي هر حمله پس از مشاهده رفتار آن حمله و ثبت داده هاي مربوط به آن با تحليل هايي كه بر روي داده ها صورت مي گيرد تهيه مي گردد، بدينوسيله سيستم در آينده به راحتي آن حمله را خواهد شناخت و جلوي

[۱] Support vector machine

نفوذ و حمله به شبکه را خواهد گرفت .تحليل بر روي داده ها جهت استخراج امضا توسط افراد خبره صورت مي گرفت ولي جديداً در اين حوزه نيز از داده كاوي استفاده مي گردد .
(بلدرن، تالبوت و دبار ۲۰۰٦)هدف از ضمانت اطلاعات، محرمانه نگه داشتن اطلاعات و کنترل سطح دسترسی معرفی نمودند که اطلاعات خاص فقط توسط کاربران مجاز قابل دسترسی می باشد وکاربرد سیستم امنیتی تشخیص وجلوگیری از وقایع نامطلوب می باشد. بطور کلی سیستم نفوذ شامل ۳ عملکرد (نظارت، کشف، واکنش) است. تشخیص وقایع در امنیت شبکه توسط روشی از داده کاوی با عنوان یادگیری ماشین صورت گرفته است.

(هوگ ،موکیت و بیکاس ۲۰۱۲) روشهای انتخاب معيار هاي ارزيابي كارايی مورد بررسی قراردادند. براي ارزيابي و مقايسه كارايي الگوريتم ها از دومعيار استفاده شده است. برای برچسب گذاري از روش مبتني بر فاصله استفاده شده كه در اين روش خوشه هايي كه از ساير خوشه ها جدا افتاده اند و فاصله آنها از ساير خوشه ها زياد است به عنوان خوشه هاي غير نرمال و يا حمله تلقي مي‌شوند و خوشه هاي نزديك به هم شامل داده هاي نرمال هستند. اين معيارها نرخ كشف (DR) و نرخ مثبت كاذب (FPR) هستند كه پس از تشكيل ماتريس پراكندگي براي خوشه ها قابل محاسبه هستند.

(مالوف۲۰۰٦)در شبکه MITRE از روشهای داده کاوی برای بهبود فرآیند شبکه استفاده می کند و پیش زمینه ای درخصوص شبکه MITRE و ویژگی های اصلی شبکه شامل : انتخاب، تراکم، طبقه بندی و فرآیند رتبه بندی ارائه کرده است. هدف این مقاله تشخیص آنومالی وکاهش تعداد نرخ آلارم کاذب که توسط سنسورهایی در شبکه ایجاد شده برای تشخیص هشدارهای غیر ضروری می باشد. و بدین منظور از ترکیب دو روش درخت تصمیم و دسته بندی K-MEANS استفاده شده است.

(هوگ ،موکیت و بیکاس ۲۰۱۲) برای سیستم تشخیص نفوذ با استفاده از الگوریتم ژنتیک با کارایی شناسایی انواع مختلف نفوذ شبکه ارائه کردند، برای پیاده سازی و اندازه گیری عملکرد سیستم از استاندارد KDD99 استفاده شده است و برای اندازه گیری تابع برازش کروموزوم از معادله انحراف با فاصله استفاده شده است. نرخ تشخیص و فرایند تا حد زیادی بهبود داده شده ونرخ مثبت کاذب بسیار کاهش یافته است.

۱-۳-هدف و موضوع تحقیق

هدف از این پایان نامه آشنایی با روشهای تشخیص نفوذ ، بررسی سیستمهای تشخیص نفوذ ، بررسی روشهای داده کاوی در تشخیص نفوذ، و در نهایت ارائه روش جدید با رویکرد مبتنی بر الگوریتم ژنتیک بنام Gene Experssion Programming در تشخیص نفوذ مورد استفاده قرار می گیرد.

۱-۴- نتایج حاصل شده

در این پایان نامه با ارائه مدل جدیدی از الگوریتم GEP برای دسته بندی رکوردهای اطلاعاتی شبکه به منظور انجام فرآیند تشخیص نفوذ استفاده می شود و با تکیه بر مجموعه داده استاندارد KDDCUP99 به مطالعه انواع حملات می پردازیم.

۱-۵- مروری بر فصول پایان نامه

این پایان نامه مشتمل بر پنج فصل است . درفصل دوم روش های استفاده شده در تشخیص نفوذ معرفی می شود.
در فصل سوم مفاهیم داده کاوی بررسی شده است و سعی شده است تمامی موارد مربوط به داده کاوی بصورت خلاصه پوشش داده شود.
در فصل چهارم مفاهیم و الگوریتم های یادگیری ماشین ذکر شده است و به طور کامل مفاهیم الگوریتم ژنتیک توضیح داده شده است .
در فصل پنجم روشی بر مبنای الگوریتم برنامه نویسی بیان ژن (GEP) پیشنهاد شده است . همچنین در این فصل به طور کامل الگوریتم GEP توضیح داده شده است و گام های پیاده سازی تشریح شده است . در نهایت نتایج حاصل از اجرای الگوریتم بروی مجموعه حملات داده استاندارد KDDCUP99 نشان داده شده است.

فصل دوم

سیستم های تشخیص نفوذ

۲ـ۱ـ مقدمه

سیستمی دارای امنیت است که بتوان نسبت به عملکرد آن اعتماد نمود. به منظور رسیدن به درجه ی بالای اعتماد معمولاً سیاستهای امنیتی درنظر گرفته می شود. این سیاست ها عملکرد بخش های مختلف سیستم را کنترل کرده و نیازمندی های لازم جهت اعمال نظارت را مشخص می کنند. تعریفی دقیق از سیستم کامپیوتری امن به این صورت است: سیستمی امن است که بتواند محرمانگی ، جامعیت و در دسترس بودن را برای کاربران خود فراهم آورد. محرمانگی به این معنی است که اطلاعاتی فقط در اختیار افرادی قرار گیرد که مجوز دسترسی به آن داده ها را قبلاً از مدیر سیستم داشته باشند.
جامعیت بدین معنی است که اطلاعات در اثر حوادث و یا فعالیتهای خرابکارانه بدون کوچکترین تغییر باقی بمانند و در دسترس بودن نیز بدین معنی است که سیستم باید در مواقع نیاز فعال بوده و بدون هیچ مشکلی منابع و اطلاعات را در اختیار استفاده کنندگان قرار دهد. در جوامع امروز سرعت دسترسی به اطلاعات و پردازش سریع آنها یک نیاز بدیهی است . این نیازمندی باعث شده است که اطلاعات بیشتری در سیستم های کامپیوتری ذخیره و بازیابی شوند و برای استفاده از این اطلاعات نیازمند به اشتراک گذاردن آنها هستیم . به همین دلیل شبکه های کامپیوتری به سرعت در حال رشد و تکامل هستند.
با افزایش دانش مربوط به چگونگی عملکرد شبکه ها و برنامه ها ی کامپیوتری ، نفوذکنندگان ضعف های سیستم را به خوبی شناسایی کرده و از آنها برای نفوذ به شبکه استفاده می کنند. در برخی از موارد این ضعف ها به گونه ای است که نفوذ کننده را قادر می سازد هر عمل دلخواه را در سیستم انجام دهد . نفوذگرها ممکن است از الگوهای خاص نفوذ استفاده کنند که ردیابی و شناسایی آنها بسیار مشکل است . همچنین یک نفوذگر ماهر ابتدا برخی حرکات فریبنده انجام می دهد و آنگاه در فرصت مناسب حمله اصلی را به اجرا در می آورد و در برخی از موارد نفوذگرها با پنهان کردن ردپای خود کار تشخیص نفوذ را بسیار مشکل می کنند. (مالوف۲۰۰٦).

نفوذتوسط سه گروه صورت می گیرد: الف) حمله کنندگان که از طریق اینترنت دسترسی پیدا می کنند.
ب) کاربران مجازي که در تلاش براي کسب دسترسی بیشتري هستند، در حالیکه اجازه چنین کاري ندارند.
ج) کاربران مجازي که از دسترسی خود سوء استفاده می کنند.

سیستم تشخیص نفوذ ابزار سخت افزاري یا نرم افزاري است که این تحلیل را خودکار انجام می دهد(طاهري منفرد۱۳۸۷).
براي ایجاد امنیت کامل در يك سیستم کامپیوتري، علاوه بر دیواره هاي آتش(Firewall) و دیگر تجهیزات جلوگیري از نفوذ، سیستمهاي دیگري به نام سیستم هاي تشخیص نفوذ (IDS)[۲] مورد نیاز مي باشند تا بتوانند در صورتي که نفوذگر از دیواره ي آتش، آنتي ویروس و دیگر تجهیزات امنیتي عبور کرد و وارد سیستم شد، آن را تشخیص داده و چار ه اي براي مقابله با آن بي اندیشند .سیستم هاي تشخیص نفوذ را مي توان از

[۲] Intrusion Detection System (IDS)

سه جنبه ي روش تشخيص، معماري و نحوه ي پاسخ به نفوذ طبقه بندي كرد .انواع مختلفي از معماري سيستمهاي تشخيص نفوذ وجود دارد كه به طور كلي مي توان آن ها را در سه دسته ي مبتني بر ميزبان (HIDS)[۳] ، مبتني بر شبكه (NIDS)[٤] و توزيع شده (DIDS)[٥] تقسيم بندي نمود.

۲-۲- دلايل استفاده از سيستم تشخيص نفوذ

دلايل متعددي را براي لزوم استفاده ازIDS ميتوان نام برد كه اهم آنها در ادامه آمده است :

الف) تشخيص حمله و ساير فعاليتهاي خصمانه براي نقض امنيت ميزبان كه ديگر مكانيزمهاي امنيتی با آن مقابله نكرده اند.

ب) شناسايی و مقابله با فعاليتهاي پيش نياز براي حمله

ج)گزارش خطرات موجود به سازمان

د) كنترل كيفيت طرح امنيتی و مديريتی، بخصوص براي سازمانهاي بزرگ و پيچيده

ه) تامين اطلاعات مفيد درباره ي نفوذهايی كه رخ داده است .اين كار باعث بهبود شناسايی، بازيابی و تصحيح دلايل نفوذ می شود.

۲-۳- نگاهي بر سيستمهاي تشخيص نفوذ (IDS)

سيستمهاي تشخيص نفوذ (IDS) وظيفه ي شناسايي و تشخيص هر گونه استفاده ي غيرمجاز به سيستم، سوء استفاده و يا آسيب رساني توسط هر دو دسته ي كاربران داخلي و خارجي را بر عهده دارند .سيستم هاي تشخيص نفوذ به صورت سيستم هاي نرم افزاري و سخت افزاري ايجاد شده و هر كدام مزايا و معايب خاص خود را دارند .سرعت و دقت از مزاياي سيستمهاي سخت افزاري است و عدم شكست امنيتي آن ها توسط نفوذگران، قابليت ديگر اين گونه سيستم ها مي باشد .اما استفاده ي آسان از نرم افزار، قابليت انطباق پذيري در شرايط نرم افزاري وتفاوت سيستم هاي عامل مختلف، عموميت بيشتري را به سيستمهاي نرم افزاري مي دهد و عموماً اين گونه سيستم ها انتخاب مناسب تري هستند.

به طور كلي سه عملكرد اصلي IDS عبارتند از:

۱- ارزيابی و نظارت ۲- كشف ۳- واكنش

بر همين اساس هرIDS را مي توان براساس روشهاي تشخيص نفوذ، معماري و انواع پاسخ به نفوذ دسته بندي كرد.

۲-٤- انواع روشهاي تشخيص نفوذ

نفوذ به مجموعه ي اقدامات غيرقانوني كه صحت و محرمانگي و يا دسترسي به يك منبع را به خطر مي اندازد، اطلاق مي گردد .نفوذ ها مي توانند به دو دسته ي داخلي و خارجي تقسيم شوند .نفوذهاي خارجي به آن دسته نفوذهايي گفته مي شود كه توسط افراد مجاز و يا غيرمجاز از خارج شبكه به درون شبكه ي داخلي صورت مي گيرد و نفوذهاي داخلي توسط افراد مجاز در سيستم و شبكه ي داخلي، از درون خود شبكه انجام مي پذيرد.

نفوذ گرها عموماً از عيوب نرم افزاري، شكستن كلمات رمز، استراق سمع ترافيك شبكه و نقاط ضعف طراحي در شبكه، سرويس ها و يا كامپيوترهاي شبكه براي نفوذ به سيستم ها و شبكه هاي كامپيوتري بهره

---

[۳] Host-based Intrusion Detection System (HIDS)

[٤] Network-based Intrusion Detection System (NIDS)

[٥] Distributed Intrusion Detection System (DIDS)

مي برند.به منظور مقابله با نفوذگران به سيستم ها و شبكه هاي كامپيوتري، روش هاي متعددي تحت عنوان روشهاي تشخيص نفوذ ايجاد گرديده است كه عمل نظارت بر وقايع اتفاق افتاده در يك سيستم يا شبكه ي كامپيوتري را بر عهده دارد .روش هاي تشخيص مورد استفاده در سيستم هاي تشخيص نفوذ به دو دسته تقسيم مي شوند:

١ - روش تشخيص رفتار غير عادي

٢-روش تشخيص سوءاستفاده يا تشخيص مبتني بر امضاء

٢-٤-١- روش تشخيص رفتار غير عادي

در اين روش، يك نما از رفتار عادي ايجاد مي شود .يك ناهنجاري ممكن است نشان دهنده ي يك نفوذ باشد. براي ايجاد نماهاي رفتار عادي از رويكردهايي از قبيل شبكه هاي عصبي، تكنيك هاي يادگيري ماشين و ... استفاده مي شود.

براي تشخيص رفتار غيرعادي، بايد رفتارهاي عادي را شناسايي كرده والگوها وقواعد خاصي براي آن ها پيدا كرد.رفتارهايي كه از اين الگوها پيروي مي كنند، عادي بوده و رويدادهايي كه انحرافي بيش از حد معمول آماري از اين الگوها دارند، به عنوان رفتار غيرعادي تشخيص داده مي شود .نفوذهاي غيرعادي براي تشخيص بسيار سخت هستند، چون هيچگونه الگوي ثابتي براي نظارت وجود ندارد .معمولاً رويدادي كه بسيار بيشتر يا كمتر از دو استاندارد انحراف از آمار عادي به وقوع مي پيوندد، غيرعادي فرض مي شود .به عنوان مثال اگر كاربري به جاي يك يا دو بار ورود و خروج عادي به سيستم در طول روز، بيست بار اين كار را انجام دهد، و يا كامپيوتري كه در ساعت ٢ بعد از نيمه شب مورد استفاده قرار گرفته در حالي كه قرار نبوده كامپيوتر فوق پس از ساعت اداري روشن باشد .هر يك از اين موارد مي تواند به عنوان يك رفتار غير عادي در نظر گرفته شود.يک معياري كه در تشخيص رفتار غيرعادي به كارمي رود تشخيص سطح آستانه می باشد.

- **تشخيص سطح آستانه**

تعداد ورود/ خروج به سيستم و يا زمان استفاده از سيستم، از مشخصه هاي رفتار سيستم و يا استفاده كننده است كه ميتوان با شمارش آن به رفتار غيرعادي سيستم پي برد و آن را ناشي از يك نفوذ دانست.

٢-٤-٢- روش تشخيص سوءاستفاده يا تشخيص مبتني بر امضاء

در اين تكنيك كه معمولاًبا نام تشخيص مبتني بر امضاء شناخته شده است، الگوهاي نفوذ از پيش ساخته شده به صورت قانون نگهداري مي شوند .به طوري كه هر الگو انواع متفاوتي از يك نفوذ خاص را در بر گرفته و در صورت بروز چنين الگويي در سيستم، وقوع نفوذ اعلام مي شود .در اين روش ها، معمولاً تشخيص دهنده داراي پايگاه داده اي از امضاء ها يا الگوهاي حمله است و سعي مي كند با بررسي ترافيك شبكه، الگوهاي مشابه با آن چه را كه در پايگاه داده ي خود نگهداري مي كند، بيابد .اين دسته از روش ها تنها قادر به تشخيص نفوذهاي شناخته شده مي باشند و در صورت بروز حملات جديد در سطح شبكه، نمي توانند آن ها را شناسايي كنند و مدير شبكه بايد همواره الگوي حملات جديد را به سيستم تشخيص نفوذ اضافه كند .از مزاياي اين روش دقت در تشخيص نفوذهايي است كه الگوي آن ها عيناً به سيستم داده شده است.