



تشخیص نفوذ شبکه های کامپیوتری

Computer network interusion detection

مولفان:

مهندس سیده مریم حسینی

دانشگاه آزاد اسلامی واحد تهران شمال

دکتر ناصر مدیری

دانشگاه آزاد اسلامی واحد زنجان

عنوان: تشخیص نفوذ شبکه های کامپیوتری

مؤلف: مهندس سیده مریم حسینی - دکتر ناصر مدیری

ناشر: سنجش و دانش

نوبت چاپ: اول - ۱۳۹۹

تیراژ: ۵۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۰۵-۱۱۳۸-۰۰

نشانی: میدان انقلاب. خیابان انقلاب. خیابان دانشگاه. پلاک ۱۲۶.

تلفن: ۰۲۱۶۱۲۶۰

«کلیه حقوق مادی و معنوی این اثر محفوظ می باشد»»

سنجش و دانش

www.sanjesh.ir

sanjeshodanesh@iran.ir

قیمت: ۳۵۰۰۰ ریال



www.ketab.ir

فهرست مطالب

۱	پیشگفتار
۲	مقدمه
۴	فصل اول
۴	کلیات
۵	اهداف
۵	اهداف بزرگ
۶	پیشینه
۱۱	روش بررسی موضوع
۱۲	فصل دوم
۱۲	سیستم تشخیص نفوذ و تکنیک‌های آن
۱۳	نفوذ چیست و انواع آن کدامند؟
۱۳	نفوذگر کیست؟
۱۴	روش های نفوذ به شبکه های کامپیوتری
۱۴	استفاده از عیوب نرم افزاری
۱۴	شکستن کلمه عبور
۱۵	استراق سمع ترافیک نا امن
۱۵	استفاده از نقاط ضعف طراحی
۱۶	تشخیص نفوذ
۱۶	سیستم تشخیص نفوذ
۱۸	اجزای تشکیل دهنده سیستم های تشخیص نفوذ IDS
۲۲	روش های تشخیص نفوذ
۲۲	شناسایی امضاء یا (SIGNATURE)
۲۳	تشخیص رفتار غیر عادی (ناهنجاری)
۲۵	تشخیص پرتکل غیرعادی (ANOMALY PROTOCOL)
۲۶	انواع معماری های تشخیص نفوذ
۲۶	سیستم تشخیص نفوذ مبتنی بر میزبان
۲۸	سیستم تشخیص نفوذ مبتنی بر شبکه

- ۳۰.....: معایب NIDS
- ۳۱.....: مزیت‌های NIDS
- ۳۲.....: وظایف اصلی NIDS
- ۳۳.....: سیستم تشخیص نفوذ توزیع شده:
- ۳۴.....: روش‌های برخورد و پاسخ به نفوذ:
- ۳۵.....: پاسخ غیرفعال در سامانه تشخیص نفوذ:
- ۳۵.....: پاسخ فعال در سامانه تشخیص نفوذ:
- ۳۶.....: اهداف سیستم‌های تشخیص نفوذ:
- ۳۷.....: قابلیت‌های IDS
- ۳۷.....: جایگزین‌های IDS
- ۳۸.....: محدودیت‌های سیستم‌های تشخیص نفوذ:
- ۳۹.....: معرفی چند نمونه سیستم تشخیص نفوذ:
- ۴۱.....: مقایسه سیستم‌های تشخیص نفوذ:
- ۴۳.....: سیستم جلوگیری از نفوذ (IPS)
- ۴۴.....: IPS‌ها چگونه فعالیت‌های مخرب را شناسایی می‌کنند؟
- ۴۵.....: IPS‌ها به چهار دسته تقسیم می‌شوند:
- ۴۷.....: IPS یک راه کار امنیتی فعال:
- ۴۷.....: IDS یا IPS کدامیک؟
- ۴۸.....: روش کار IDS و IPS:
- ۴۹.....: تفاوت IDS و IPS و فایروال:
- ۵۱.....: جلوگیری از نشت اطلاعات: (DLP)
- ۵۲.....: هفت گام مفید در جلوگیری از نشت اطلاعات:
- ۵۴.....: فرایندهای جلوگیری از نشت اطلاعات: (DLP)
- ۵۸.....: فصل سوم:
- ۵۸.....: داده کاوی:
- ۶۰.....: تاریخچه داده کاوی:
- ۶۱.....: فرایند داده کاوی:
- ۶۳.....: مزایا و معایب داده کاوی:
- ۶۳.....: مزایای داده کاوی:

۶۴.....	معایب داده کاوی :
۶۵.....	کاربردهای داده کاوی :
۶۶.....	کسب و کار.....
۶۶.....	پژوهش های زنوم :
۶۷.....	بازاریابی اطلاعات :
۶۷.....	سیستم های ارتباطی :
۶۷.....	تکنیکهای داده کاوی :
۶۸.....	دسته بندی.....
۶۸.....	خوشه بندی.....
۷۳.....	فصل چهارم.....
۷۳.....	رگرسیون گیری :
۷۳.....	تجمع و همبستگی :
۷۴.....	درخت تصمیم گیری :
۷۴.....	ویزگیهای درخت تصمیم.....
۷۵.....	شبکه های بیزین.....
۷۶.....	منطق فازی.....
۷۷.....	روشهای آماری.....
۷۸.....	الگوریتم ماشین بردار پشتیبان (SVM).....
۷۹.....	مقایسه روشهای داده کاوی مورد استفاده در تشخیص نفوذ.....
۸۱.....	شبکه های عصبی مصنوعی :
۸۵.....	یادگیری شبکه.....
۸۷.....	شبکه عصبی چند لایه (MLP).....
۸۸.....	قانون یادگیری پس انتشار خطا BP'.....
۸۸.....	الگوریتم ژنتیک.....
۹۱.....	ساختار الگوریتم های ژنتیکی.....
۹۲.....	عملگرهای ژنتیکی.....
۹۴.....	روند کلی الگوریتم های ژنتیکی.....
۹۶.....	فصل پنجم.....
۹۶.....	نتیجه گیری.....

پیشگفتار:

با رشد فناوری اطلاعات امنیت، شبکه به عنوان یکی از مباحث مهم و چالش بسیار بزرگ مطرح است. سیستم های تشخیص نفوذ مولفه اصلی یک شبکه امن است. سیستم های تشخیص نفوذ سنتی نمی توانند خود را با حملات جدید تطبیق دهند از این رو سیستم های تشخیص نفوذ مبتنی بر داده کاوی امروزه پیشنهاد می شود. مشخص نمودن الگوهایی در حجم زیاد داده، کمک بسیار بزرگی به ما می کند. متدهای داده کاوی با مشخص نمودن یک برچسب دودودی (بسته نرمال، بسته ناهنجار) و همچنین مشخص نمودن ویژگی ها و خصیصه با الگوریتم های دسته بندی می تواند داده غیرنرمال را تشخیص دهند. از همین رو دقت و درستی سیستم های تشخیص نفوذ افزایش یافته. روابط امنیت شبکه بالا می رود. در این روش ما الگوریتم های مختلف شبکه و شبکه عصبی را روی مجموعه داده خود تست خواهیم کرد. امروزه تهدیداتی که از اینترنت می آیند بیش از پیش پدید شده و توانایی این را دارند که از راه حل های امنیتی معمول از قبیل دیوار آتش ها و آنتی ویروس ها، بگریزند. یک راه حل ممکن برای بهبود امنیت، اضافه کردن یک سیستم تشخیص نفوذ است که بعنوان یک لایه اضافی در راه حل های امنیتی محسوب میشود. هدف از تشخیص نفوذ، شناسایی فعالیت های غیرعادی است که قصد استفاده غیرمجاز، آسیب رساندن به سیستم ها و سوءاستفاده از شبکه های کامپیوتری را دارند. در این میان، روش های متعددی توسط محققین ارائه شده است که هر یک به نوبه خود عملکردی را روی رویه رشدی داشته اند. اما با توجه به حجم عظیم داده ها در هر سازمان مبتنی بر شبکه، مثل شبکه های مخابراتی، بررسی و تحلیل ترافیک موجود به صورت دستی کاری دشوار، کم دقت و زمانبری است. با این وجود با بهره گیری از تکنیک های دسته بندی در زمینه داده کاوی با استفاده از شبکه عصبی و الگوریتم ژنتیک می توان به تحلیل خودکار و تشخیص امنیت شبکه پرداخت.