

۲۰۹۷۸.۸



نقش داده کاوی در سیستم‌های

تشخیص نفوذ

مؤلفان:

هادی بارانی برواتی

اطهره حاجی زاده مطلق

سرشناسه	: بارانی برواتی، هادی، ۱۳۶۰-
عنوان و نام پدیدآور	: نقش داده کاوی در سیستم های تشخیص نفوذ/ مولفان هادی بارانی برواتی، اطهره حاجی زاده مطلق.
مشخصات نشر	: تهران: انتشارات راه دکتري: سنجش و دانش، ۱۳۹۸.
مشخصات ظاهري	: ۹۸ص.
شابک	: 978-622-241-305-7
وضعیت فهرست نویسی	: فیپا
موضوع	: سامانه های تشخیص نفوذ (ایمن سازی کامپیوتر) -- ایران -- نمونه پژوهی
موضوع	: Intrusion detection systems (Computer security) -- Iran -- Case studies
موضوع	: شبکه های کامپیوتری -- ایران -- تدابیر ایمنی -- نمونه پژوهی
موضوع	: Computer networks -- Iran -- Security measures -- Case studies
موضوع	: داده کاوی -- نمونه پژوهی
موضوع	: Data mining -- Case studies
شناسه افزوده	: حاجی زاد مطلق، اطهره، ۱۳۶۲-
رده بندی کنگره	: ۵۹/۷۰۵Tf
رده بندی دیویی	: ۸/۰۰۵
شماره کتابشناسی ملی	: ۸۸۸۴۶۷

www.sanjesh.ir

عنوان: نقش داده کاوی در سیستم های تشخیص نفوذ

مولفان: هادی بارانی برواتی، اطهره حاجی زاده مطلق

ناشر: انتشارات سنجش و دانش

نوبت چاپ: اول ۱۳۹۸

تیراژ: ۵۰۰ نسخه

بهاء: ۳۰۰۰۰۰ ریال

مرکز بخش: تهران، خیابان انقلاب، خیابان دانشگاه، پلاک ۱۲۶

تلفن تماس: ۰۲۱-۶۱۲۶

پیشگفتار

در این کتاب یک رویکرد برخط برای مدیریت هشدارهای تولیدشده توسط سیستم‌های تشخیص نفوذ پیشنهاد می‌شود. همزمان با پیشرفت و گسترش روزافزون اینترنت و کاربردهای مبتنی بر آن، بر تعداد و پیچیدگی حملات سایبری نیز افزوده می‌شود. بنابراین، استفاده از ابزارهای مختلف امنیتی برای حفاظت از سیستم‌ها و شبکه‌های کامپیوتری به یک نیاز حیاتی تبدیل شده است. در میان این ابزارها، سیستم‌های تشخیص نفوذ از مؤلفه‌های ضروری دفاع در عمق می‌باشند. یکی از بزرگ‌ترین مشکلات سیستم‌های تشخیص نفوذ، تولید سیلی از هشدارهاست. هشدارهایی که اغلب آن‌ها هشدارهای غلط، تکراری، و بی‌اهمیت هستند. در میان رویکردهای مختلف برای حل این مشکل، روش‌های داده‌کاوی از سوی بسیاری از محققان پیشنهاد شده است. با این حال، بسیاری از روش‌های قبلی نتوانسته‌اند مشکلات را به طور کامل حل کنند. به علاوه اغلب روش‌های پیشین، از مشکلاتی نظیر وابستگی به نیروی انسانی و برون خط بودن رنج می‌برند. رویکرد پیشنهادی، قابلیت دریافت هشدارهایی از چندین سیستم تشخیص نفوذ را داراست. ارزیابی‌های انجام شده نشان می‌دهد که راهکار ارائه شده با کاهش حجم هشدارها به میزان ۹۴.۳۲٪، می‌تواند تأثیر بسزایی در مدیریت هشدارها داشته باشد. این رهیافت، به دلیل استفاده از رویکرد تجمعی داده‌کاوی و به‌کارگیری الگوریتم‌های بهینه، می‌تواند متخصص امنیت شبکه را به صورت برخط، از وضعیت شبکه‌ی تحت نظارت، آگاه سازد.

۱.....	فصل اول	۱
۱.....	مقدمه	۱
۲.....	مقدمه	۲
۲.....	سیستم های تشخیص نفوذ	۲
۶.....	کاربردها	۶
۷.....	به کارگیری ترکیبی روش های داده کاوی	۷
۸.....	فصل دوم	۸
۸.....	مروری بر مفاهیم اولیه	۸
۹.....	امنیت شبکه های	۹
۱۲.....	دسته بندی سیستم های تشخیص نفوذ بر اساس نوع منبع داده	۱۲
۱۳.....	دسته بندی سیستم های تشخیص نفوذ بر اساس روش های مختلف تشخیص	۱۳
۱۴.....	دسته بندی سیستم های تشخیص نفوذ بر اساس نحوه انتشار به نفوذ	۱۴
۱۵.....	دسته بندی سیستم های تشخیص نفوذ بر اساس معماری	۱۵
۱۸.....	داده کاوی	۱۸
۲۰.....	تشخیص نفوذ و داده کاوی	۲۰
۲۳.....	قوانین انجمنی	۲۳
۲۴.....	قوانین سریالی مکرر	۲۴
۲۶.....	دسته بندی	۲۶
۲۷.....	خوشه بندی	۲۷
۲۸.....	جمع بندی این فصل	۲۸
۳۰.....	فصل سوم	۳۰
۳۰.....	مروری بر کارهای انجام شده	۳۰

۳۱	تکنیک‌های پردازش هشدارها
۴۵	فرآیند بهبود کیفیت هشدارها
۴۸	فصل چهارم
۴۸	معرفی رویکرد پیشنهادی
۴۹	معماری رویکرد پیشنهادی
۵۱	قالب استاندارد هشدارها در رویکرد پیشنهادی
۵۲	مؤلفه‌های کارکردی رویکرد پیشنهادی
۵۲	مؤلفه‌ی بهنجاری
۵۳	مؤلفه‌ی پیش‌پردازش
۵۴	مؤلفه‌ی همجوشی
۵۷	مؤلفه‌ی واریاسیون
۵۸	مؤلفه‌ی کاهش هشدارهای غلط
۵۹	مؤلفه‌ی شناسایی هشدارهای رایج
۶۰	مؤلفه‌ی تجمیع
۶۴	جمع‌بندی این فصل
۶۵	فصل پنجم
۶۵	آزمایش‌ها و ارزیابی رویکرد پیشنهادی
۶۶	مقدمه
۶۶	مجموعه داده‌ی ارزیابی
۶۷	مجموعه‌های داده‌ی DARPA-LINCOLN و مجموعه داده‌ی KDD99
۷۰	داده‌های INTERNET EXPLORATION SHOOTOUT DATASET
۷۰	سایر مجموعه داده‌های رایج
۷۱	مجموعه داده‌های تولیدشده‌ی دیگر
۷۲	معیارهای ارزیابی کارایی

۷۴	IDS مورد استفاده جهت ارزیابی.....
۷۵	پیاده‌سازی آزمایشی رویکرد پیشنهادی.....
۷۵	نتایج ارزیابی با استفاده از مجموعه داده‌ی DARPA 1999.....
۷۹	نتایج ارزیابی در محیط شبکه‌ی واقعی.....
۸۱	نتایج مقایسه‌ی راهکار پیشنهادی با کارهای پیشین.....
۸۲	جمع‌بندی این فصل.....
۸۳	مراجع.....
۸۸	واژه‌نامه.....