



- پاکروان، مهران، ۱۳۵۵ - :
ارائه روشی مبتنی بر کاهش ویژگی برای بهبود تشخیص نفوذ در شبکه با استفاده از دادگان kdd cup / مولف مهران پاکروان،
تهران: سنجش و دانش، ۱۴۰۰.
ز، ۹۹ ص:؛ مصور: (بخشی رنگی)، نمودار (بخشی رنگی).
978-622-05-2926-2
فیبا
وضعیت فهرست نویسی
پادداشت
موضوع
کتابنامه: ص، ۹۹-۹۹.
آزمایش نفوذ (امن سازی کامپیوتر)
Penetration testing (Computer security)
کامپیوترها - ایمنی اطلاعات - مدیریت
Computer security -- Management
هکرها
Hackers
نرم افزار - آزمایش
Computer software -- Testing
شبکه های کامپیوتری -- تدابیر ایمنی
Computer networks -- Security measures
شبکه های کامپیوتری -- تدابیر ایمنی - نرم افزار
Computer networks -- Security measures -- Software
QAV۶/۹
۰۰۵/۸
۸۷۸۳۳۳۹
فیبا

رده بندی کنگره

رده بندی دیویی

شماره کتابشناسی ملی

اطلاعات رکورد کتابشناسی

عنوان : ارائه روشی مبتنی بر کاهش ویژگی برای بهبود تشخیص نفوذ
ذ در شبکه با استفاده از دادگان kdd cup

مؤلف :مهران پاکروان

ناشر : سنجش و دانش

نوبت چاپ : چاپ اول - ۱۴۰۰

تیراژ : ۳۰ نسخه

شابک : ۹۷۸-۶۲۲-۰۵-۲۹۲۶-۲

نشانی : میدان انقلاب . خیابان انقلاب . خیابان دانشگاه . پلاک ۱۲۶ . تلفن : ۲۱۶۱۲۶

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

سنجش و دانش

www.sanjesh.ir
sanjeshodanesh@iran.

قیمت : ۲۵۰۰۰۰ ریال

پیشگفتار

امروزه پیشرفت در تکنولوژی اجازه می دهد تا کامپیوترها از راه دور مدیریت شوند و از این راه بزرگراهی برای همه انواع اطلاعات از طریق اینترنت فراهم شده است. اینترنت امروز به دلیل تهدیدهای گوناگون سایبری به طور فزاینده‌ای در معرض خطر قرار گرفته است و میزان و پیچیدگی حملات سایبری به طور نگران کننده ای در حال رشد است. هکرها تکنیکهای جدیدی را به صورت روزانه برای دور زدن لایه‌های امنیتی اختراع کرده و مورد استفاده قرار می دهند. سیستم های تشخیص نفوذ به کشف و شناسایی رفتارهای غیر مجاز سیستم، مانند استفاده، کپی کردن، تغییر و تخریب کمک می کنند. با ظهور تکنیک های هوش مصنوعی، رویکردهای یادگیری محور برای تشخیص حملات سایبری، بیشتر بهبود و گسترش یافته اند و در بسیاری از مطالعات به نتایج قابل توجهی دست یافته اند. در این کتاب از تئوری بازی ها برای تشخیص و انتخاب ویژگی های موثر استفاده شده است. همچنین ادامه برای کلاسه بندی از تکنیک XGBoost استفاده شد. نتایج نشان می دهد که روش پیشنهادی از نظر پارامترهای ارزیابی نسبت به سایر روش ها بهتر عمل کرده است.

فهرست مطالب

۱	فصل اول
۱	مقدمه
۲	مقدمه
۴	بیان موضوع
۸	اهمیت و ضرورت پرداختن به موضوع
۹	اهداف
۹	مفروضات
۱۰	نحوه پرداختن به موضوع
۱۳	فصل دوم
۱۳	مبانی نظری
۱۳	و مروری بر پژوهش های پیشین
۱۴	نفوذ
۱۸	تشخیص سوءاستفاده یا تشخیص مبتنی بر امضاء
۱۹	کاهش ابعاد ویژگی
۲۱	آماده سازی داده ها
۲۲	فهم داده
۲۳	پاک سازی داده
۲۳	یکپارچه سازی داده
۲۴	تبدیل داده
۲۵	تخلیص داده ها
۲۶	انتخاب ویژگی ها
۳۱	الگوریتمهای دسته بندی
۳۴	روش های یادگیری ماشین برای تشخیص نفوذ امنیت سایبری
۴۰	مجموعه های داده امنیتی سایبری برای ML و DM
۴۱	داده سطح بسته

۴۳	 داده NetFlow
۴۶	 مجموعه‌های داده عمومی
۴۹	 مروری بر تحقیقات پیشین
۶۱	 فصل سوم
۶۱	 مبانی نظری مدل‌سازی
۶۱	 و روش پیشنهادی
۶۲	 روش پیشنهادی
۶۴	 کاهش ابعاد با تئوری بازی‌های همکاری
۶۴	 مفاهیم پایه تئوری اطلاعات
۶۷	 تئوری بازی‌های همکاری
۷۲	 روش‌های کلاسه‌بندی
۷۲	 بگینگ
۷۴	 بوستینگ
۷۵	 ارتقای گرادیان XGboost
۷۸	 فصل چهارم
۷۸	 پرداختن به یافته‌ها
۷۹	 ابزار
۷۹	 رایانه و سیستم عامل
۸۰	 نرم افزار
۸۰	 پارامترهای ارزیابی
۸۴	 پایگاه داده مورد استفاده
۸۵	 تجزیه و تحلیل تاثیر ویژگی
۹۳	 جمع بندی
۹۳	 سخن آخر
۹۶	 مراجع