سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:

تشخیص حملات منع سرویس توزیع شده در شبکه های نرم افزارمحور DOR:۲۰.۱۰۰۱.۱.۲۳۲۲۴۳۴۷.۱۴۰۰.۹.۱.۴.۱

محل انتشار:

فصلنامه پدافند الکترونیکی و سایبری, دوره 9, شماره 1 (سال: 1400)

تعداد صفحات اصل مقاله: 18

نویسندگان:

افسانه بنی طالبی دهکردی - *دانشگاه آزاداسلامی،واحداصفهان(خوراسگان)،اصفهان،ایران*

محمدرضا سلطان آقایی - *دانشگاه آزاداسلامی،واحداصفهان(خوراسگان)،اصفهان،ایران*

فرساد زمانی بروجنی - *دانشگاه آزاداسلامی،واحداصفهان(خوراسگان)،اصفهان،ایران*

خلاصه مقاله:

شبکه های نرم افزارمحور، معماری جدیدی از شبکه های کامپیوتری بوده که از هدایت کننده مرکزی استفاده می کنند. این شبکه ها متکی بر نرم افزار هستند و از این رو، حملات امنیتی گوناگونی می تواند از طریق اجزای مختلف شبکه بر ضد آن ها صورت گیرد. یکی از این نوع حملات، حمله منع سرویس توزیع شده است. این حمله یکی از جدی ترین تهدیدات در دنیای شبکه های کامپیوتری است و بر روی کارایی شبکه، تاثیرمی گذارد. در این پژوهش یک روش تشخیص حملات منع سرویس توزیع شده به نام «حمله یاب» در شبکه های نرم افزارمحور ارائه شده است. این سامانه مبتنی بر ترکیب روش های آماری و یادگیری ماشین است. در روش آماری از آنتروپی مبتنی بر آی پی مقصد و توزیع نرمال با استفاده از حد آستانه انعطاف پذیر، برای تشخیص حملات استفاده شده است، توزیع نرمال، یکی از مهم ترین توزیع های احتمال پیوسته در نظریه احتمالات است. در این توزیع، میانگین آنتروپی و انحراف استاندارد در تشخیص حملات تاثیر دارند. در بخش یادگیری ماشین، با استخراج ویژگی های مناسب و استفاده از الگوریتم های کلاس بندی نظارت شده، دقت تشخیص حملات منع سرویس توزیع شده بالا می رود. مجموعه داده های مورد استفاده در این پژوهش، ISCX-CTU-۱۳، ISCX-IDS۲۰۱۲، SlowDDoS۲۰۱۶ و ISOT هستند. روش پیشنهادی حمله یاب با چند روش دیگر مقایسه شده است که نتیجه مقایسه نشان می دهد که روش حمله یاب با دقت ۶۵/۹۹ و نرخ هشدار غلط، ۱۲/۰ برای مجموعه داده UNB-ISCX و دقت تشخیص ۹۹/۸۴ و نرخ هشدار غلط ۰/۲۵ برای مجموعه داده CTU-۱۳ دقت و کارایی بالایی نسبت به سایر روش های دیگر دارد.

کلمات کلیدی:

حملات منع سرویس توزیع شده, شبکه های نرم افزارمحور, آنتروپی, توزیع نرمال, الگوریتم های کلاس بندی

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1203799