جامعة الموصل

كلية الهندسة

دراسة وتصميم نظام لكشف المتطفلين IDS باستخدام خوارزمية تعلم الآلة

حنين رافد محمود

مشروع دبلوم عالي في

علوم الهندسة الكهربائية

بإشراف

الدكتور

محمد يونس ذنون

١٤٤١ هـ ٢٠١٩ م

الملخص

أدى النمو الواسع للإنترنت وزيادة حجم البيانات المرسلة والمستلمة إلى ظهور أشخاص متطفلين يهدفون إلى القيام بسرقة البيانات ومنع المستخدمين الحقيقين من الدخول إلى موقع معين، إذ يستهدفون الشركات العملاقة. وقد تخسر الشركات ملايين أو مليارات الدولارات نتيجة للتوقف عن العمل بسبب هجوم Distributed Denial of Service attack (DDoS) ، وقد يخسر أصحاب الأعمال الصغيرة الكثير أيضاً.

من هنا ظهرت الحاجة إلى أنظمة كشف تطفل، ويهدف هذا المشروع إلى تصميم وبناء نظام كشف تطفل، يكشف هجمات المتطفلين وتصنيفها إلى أربعة أنواع باستخدام طريقة حذف الميزات المتكررة Recursive Feature Elimination (RFE) التي تقوم بحذف الميزات إلى ان يستخدم أقل عدد من الميزات، وتوصل المشروع إلى انه من الممكن اختيار عدد من الميزات من مجموع 41 ميزة تكون كافية لكشف الهجمات بأنواعها الأربعة وكما يأتي:
12 (ميزة لهجوم من نوع DOS) ، 15(ميزة لهجوم من نوع probe) ، 13(ميزة لهجمات R2L Remote to Local) ، 11(ميزة لهجمات U2R User to root) .
واستخدمت بيانات NSL-KDD dataset التي تتكون من مجموعتين (بيانات التدريب والاختبار) لاختبار كفاءة النموذج.

وبني النموذج باستخدام خوارزمية تعلم الآلة (خوارزمية شجرة القرار)، باستخدام لغة بايثون، وأجريت مجموعة من الاختبارات لاختبار كفاءة النموذج، وقد توصل المشروع إلى أن استخدام طريقة حذف الميزات المتكررة RFE تظهر تحسنا في أداء التصميم.

Abstract

The massive growth of the Internet and the increase in the volume of data sent and received have led to the emergence of intruders who aim to steal data and prevent real users from accessing a particular site, where they target the giants and companies may lose millions or billions of dollars as a result of downtime due to DDoS attack. Small business owner can lose a lot ,hence this led to the need of intrusion detection systems The project aims to design and build an intrusion detection system, which detects intruder attacks and classifies them into four types of attacks by using the Recursive Feature Elimination (RFE) method.

By deleting features until the lowest number of features are used, the project concluded that it is possible to select a number of features from a total of 41 features that are sufficient to detect attacks as follows 12 featur es for a DOS attack, 15 for a probe attack, 13 for R2L attacks , 11 feature for U2R attacks.

NSL-KDD dataset data set training and test data were used to test the efficiency of the model.

The model was constructed using a machine learning algorithm (decision tree algorithm) in Python and a set of tests were conducted to test the model's efficiency.

University of Mosul

College of Engineering

Electrical Engineering Department

Study and Design of Intrusion Detection System (IDS) Using Machine Learning Algorithm

Haneen Rafid Mahmood

A project in Higher diploma

in

Electrical Engineering

Supervised by

Dr.Mohammed Younis Thanoun

1441 A.H **2019 A.D.**