ACKNOWLEDGEMENT

First and foremost, I would like to thank God Almighty for giving me the strength, knowledge, ability and opportunity to undertake this research study and to persevere and complete it satisfactorily.

In my journey towards this degree, I have found teachers, friends, an inspiration, a role model and a pillar of support in my Guide. I would like to sincerely thank Dr. Faisal Mohamed Abdallah for his support and guidance and has given me invaluable guidance, inspiration and suggestions in my quest for knowledge.

My acknowledgement would be incomplete without thanking the biggest source of my strength to my family, who have been so helpful and cooperative in giving their support to help me to achieve my goals.

Abstract

Computer networks are being attacked every day. Intrusion detection systems (IDS) are used to detect and reduce effects of these attacks and it use two types of techniques signature based or anomaly based detection for detecting known and unknown attacks.

The currently used of hybrid intrusion detection systems that based on signature and anomaly based detection techniques was became inefficient for detecting attacks because it have nearly less than or equal to 95.5% for the detection rate and 1.8% for false positive rate, nowadays these values are unsatisfied for the detection so that the important of enhancing the hybrid intrusion detection system it become most needs.

In this study, the enhanced hybrid intrusion detection has been proposed to provide better results with high accuracy of the detection rate and reduce the value of false positive rate that will done by proposing new method based on decision tree of data mining techniques that is based on C4.5 algorithm via using java programming language with NSL-KDD dataset which is used weka and snort engine to detects and prevent the a portion of flooding attacks that are tested.

The results show that the proposed model is more efficient and it gives better optimum results that nearly reach to 100% for the detection rate and it's also reduces the number of false positive when it compares with previous results of intrusion detection systems.

المستخلص

نظرا لتطور الانترنت وتقنيات الحواسيب فأصبحت عمليات مهاجمة شبكات الحاسوب تتم كل يوم بالرغم من استخدام نظام الكشف عن الهجمات للكشف عن عمليات التسلل والتقليل من اثارها ويتم الكشف بأستخدام نوعين من التقنيات وذلك بالاعتماد على توقيعات وانماط معرفة مسبقا للمتسللين اوعلى تعريف سلوك المستخدمين المتحققة صحتهم لاكتشاف الهجمات المعروفة وغير المعروفة.

ان أنظمة الكشف عن الاختراق الهجينة التي تستخدم حاليًا والمبنية على تعريف انماط المتسللين او على سلوك المستخدمين المتحققة صحتهم أصبحت غير فعالة للكشف عن الهجمات لأن معدل الاكتشاف لها أقل من أو يساوى 95.5٪ و 1.8٪ لمعدل موجب الانذارات الكاذبة ، ولكن في الوقت الحاضر اصبحت هذه القيم غير مرضية للكشف عن الهجمات لذا اتت الحوجة للتعزيز من تطوير نظام كشف تسلل هجين للحصول علي نتائج اكثر فاعلية وهذا مااقتضاه هذا البحث.

يهدف هذا البحث لتحسين نظام كشف تسلل هجين للزيادة من نسبة دقة الاكتشاف وللتقليل من نسبة الانذارات الكاذبة وسوف يتم ذلك بأستخدام شجرة القرار التي هي من احدي تقنيات التنقيب لبناء خوازمية او نظرية باستخدام لغة الجافا لاكتشاف ومنع بعض من هجمات الفيضان التي اختبرت تحت استخدام ال snort and weka وعينة من بيانات الNSL-KDD dataset.

اثبتت النتائج النهائية ان نظام كشف الاختراق المقترح اكثر دقة وفعالية حيث ادى الي نتائج افضل عند مقارنتة مع النتائج السابقة ممادى الى معدل اكتشاف تبلغ نسبته تقريبا 100% وقلل ايضا من معدل الانزارات الكاذبة .

List of Contents

CHAPTER V: Conclusion And Future Work

List of Figures

List of Tables

List of Abbreviations

- DDOS attacks: Distributed Denial Of Service attacks.
- DOS attacks: Denial Of Service attacks.
- FPR : False Positive Rate
- HIDS : Hybrid Instruction Detection System.
- IDS: Instruction Detection System.
- IPS: Instruction Prevention System.
- NIDS : Network Instruction Detection System.
- NSL-KDD : Network Security laboratory Knowledge Discovery Data Mining
- SVM : Support Vector Machine.
- TPR : True Positive Rate
- Weka : Waikato Environment for Knowledge Analysis

List of Appendices