

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 توقعات وانماط معرفة مسبقا للمتسللين اوعلى تعريف سلوك المستخدمين المتحققة صحتهم لاكتشاف الهجمات المعروفة وغير المعروفة.

ان أنظمة الكشف عن الاختراق الهجينة التي تستخدم حالياً 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 الحاجة للتعزيز من تطوير نظام كشف تسلل هجين للحصول علي نتائج اكثر فاعلية وهذا ماقتضاه 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 خوارمية او نظرية بأستخدام لغة الجافا لاكتشاف ومنع بعض من هجمات الفيضان التي اختبرت تحت استخدام ال snort and weka وعينة من بيانات ال NSL-KDD dataset.

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

List of Contents

Acknowledgement	i
Abstract	ii
المستخلص.....	iii
List of Contents	iv
List of Figures	vii
List of Tables	ix
List of Abbreviations	x
List of Appendices	xi
CHAPTER I: Introduction	
1.1 Introduction	1
1.2 Problem Statements	2
1.2.1 Background	2
1.2.2 The problem	2
1.3 Importance of Research	3
1.4 Hypothesis	3
1.5 Objectives of the Research	3
1.6 Methodology	3
1.7 Boundaries	4
1.8 Contents of Research	4
CHAPTER II: Literature Review And Related Works	
2.1 Background	5
2.2 Intrusion Detection System	5
2.2.1 Deploying Intrusion Detection Systems (IDS's)	6
2.2.2 Types of Deploying IDS's	6
2.3 Techniques of Intrusion Detection System	8
2.3.1 Signature Based Detection	8
2.3.2 Anomaly Based Detection	9
2.3.3. Statefull Protocol Inspection	9

2.3.4 Hybrid Intrusion Detection Systems	10
2.4 Data Mining Techniques	10
2.4.1 Most common data mining techniques	10
2.5 Data Mining Classification Techniques	11
2.5.1 Decision Trees	11
2.6 Related Works	12
2.6.1 Evaluation of literature review and related works.....	15
CHAPTER III: Methodology	
3.1 Introduction	16
3.2 The required tools	16
3.2.1 Ubuntu	16
3.2.2 Snort	17
3.2.3 Wireshark	18
3.2.4 Weka	18
3.2.5 Dataset Description	18
3.3 Project Methodology	19
3.3.1 Reasons of using classification techniques	21
3.3.2 Reasons of using decision tree based on C4.5	21
3.4 Network Assumption	21
CHAPTER IV: Implementation And Results Analysis	
4.1 Introduction	22
4.2 Installation Steps	22
4.2.1 Installing snort packages	22
4.2.2. Configuration of snort to run as network intrusion detection system.	23
4.3 Building of signature detection model	23
4.3.1. Writing and Testing Snort's Rule.....	24
4.3.2. Load balancing on snort server	26
4.3.3. Installing and configuring BASE	28
4.4 Building of anomaly detection model	30
4.4.1 Importing and preprocessing data-set	30
4.4.2 Working of data mining algorithms	31

4.5. Testing of attacks behaviors	33
4.5.1 Nmap scanning a ttacks	33
4.5.2 SYS flooding attacks	33
4.5.3 UDP flooding attacks	35
4.5.4 HTTP Flooding attacks	36
4.6 Intrusion Prevention System	37
4.6.1 Iptables	37
4.7 Evaluation of the proposed model	40
CHAPTER V: Conclusion And Future Work	
5.1 Conclusion	41
5.2 Future Work	41
References	43

List of Figures

Figure 2.1: NIDS Network	6
Figure 2.2: HIDS Network	7
Figure 2.3: Typical Knowledge-Based IDS	8
Figure 2.4: Typical Anomaly-Based IDS	9
Figure 3.1 : Architecture of the proposed Hybrid IDS	19
Figure 3.2: Steps of building proposed Anomaly detection model	20
Figure 4.1: Information about network interface.....	24
Figure 4.2: Pinging the target	25
Figure 4.3: Detect of ICMP flooding attacks	25
Figure 4.4: Effect of ICMP flooding messages	25
Figure 4.5: Information about the db connection	27
Figure 4.6: Creation of the daemon	27
Figure 4.7: Information about barnyard	28
Figure 4.8: Interface of base module	30
Figure 4.9: Information about the interfaces and protocol.....	30
Figure 4.10: Importing of data-set	31
Figure 4.11: Removing irreverent features	31
Figure 4.12: Classification of traffics base on no of packets	32
Figure 4.13: Classification of traffics	32
Figure 4.14: Classification of TCP traffics	32
Figure 4.15: Output of scanning process	33
Figure 4.16: Result of detection nmap scanning attacks	33
Figure 4.17: Command for SYS flooding attacks	34
Figure 4.18: Result of detection SYS/TCP flooding attacks	34
Figure 4.19: Information about src and dst of messages.....	34
Figure 4.20: Effect of sys attacks on the resources	35
Figure 4.21: Effect of UDP flooding attacks on the resource.....	35
Figure 4.22: Result of detection UDP flooding attacks	36

Figure 4.23: Result of sending many no of the requests	36
Figure 4.24: Load on the target device	36
Figure 4.25: Amount of unauthorized traffics	37
Figure 4.26: Effecting of prevention mechanism after the flooding process	39
Figure 4.27: Results of classification	40

List of Tables

Table 2.1: Comparison Table	13
Table 4.1: Comparison between the previous results	40

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

APPENDIX A: Rules of signatures based detection	45
APPENDIX B: Anomaly based detection code	47