Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Diyala
College of Sciences
Department of Computer Sciences

Improvement of Intrusion Detection System Using Honeypot

A Thesis
Submitted to the Department of Computer Sciences \ College of the Sciences\ University of Diyala in a Partial Fulfillment of the Requirements for the Degree of Master in Computer Sciences

By
Ismael **S**alih **A**ref

Supervised **B**y
Prof.Dr. **Ziyad Tariq Al_Ta'i**

2018 AC *1439 AH*

بسم الله الرحمن الرحيم

" يَرفَعِ اللَّهُ الَّذِينَ آَمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ
دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ "

صدق الله العظيم

سورة المجادلة الآية (11)

Dedication

To my candles that light my life, being always with

me making me the happiest man my mother and

father with my respects and love...

To my dear brothers and sisters...

To my supervisor ...

To all my lovely family & friends...

Examination Committee Certification

We certify that we have read the thesis entitled" ***Improvement of Intrusion Detection System Using Honeypot***" presented by **(Ismael Salih Aref)** and as an examining committee, we examined the student on its contents, and in what is related to it, and that in our opinion it meets the standard of a thesis for the degree of master in Computer Science.

(Chairman)
Signature:
Name: Prof. Dr. Dhahir Abdulhade Abdullah
Date: 2/5/2019

(Member)
Signature:
Name: Assist. Prof. Dr. Jamal Mustafa Abbas
Date: 2/5/2019

(Member)
Signature:
Name: Assist. Prof. Dr. Hasanen S. Abdullah
Date: 2/5/2019

(Member/ Supervisor)
Signature:
Name: Prof. Dr . Ziyad Tariq Mustafa Al-Ta'i
Date: 2/5/2019

Approved by the Council of the College of Science

(The Dean)
Signature:
Name: Prof. Dr. Tahseen H. Mubarak
Date: 2/5/2019

Supervisor's Certification

I certify that this thesis entitled **"Improvement of Intrusion Detection System Using Honeypot"** was prepared by **"Ismael Salih Aref"** under my supervision at the University of Diyala Faculty of Science Department of computer Science , as a partial fulfillment of the requirement needed to award the degree of Master of Science in Computer Science.

(Member / Supervisor)
Signature:
Name: Prof. Dr. Ziyad Tariq Mustafa
Date: 2/5/2019

Approved by University of Diyala Faculty of Science Department of Computer Science.

Signature:
Name: Asst. Prof. Dr. Taha M. Hassan
Date: 2/5/2019
Head of Computer Science Department.

Acknowledgments

I Praise to "Allah" for mercy, unlimited help, and guidance that I needed during my study to complete my project.

Also, I would like to present my deep thanks to my supervisor, Dr. Ziyad Tariq Mustafa; for the advice and support during my research and writing of this thesis.

Thanks also go to all my friends at the University of Diyala.

Finally, I wish to express my sincere gratitude to each member of my family not only for giving me the courage to face the challenges and make my path easier but also for being so patient with me all the time.

Abstract

The computer security system is the protection of computers, which is similar to the immune system in the human body. It includes the protection of all operations and resources within the computer and the prevention of abuse by intruders. Security tools such as intrusion detection system(IDS) and honeypot trap can be used to provide protection, but each one has a shortcoming when applied alone.

In this work, An integrated system consist of IDS with a honeypot trap is proposed in order to overcome the deficiencies of each one. A C4.5 classification algorithm is used to build the detection engine of IDS. A high interaction honeypot trap is constructed and deployed to collect more details information about malicious traffics. The honeypot trap contains four services, which are HTTP, FTP, DNS, and Telnet servers. The construction of IDS passes in two stages, offline and online. In the offline stage, the IDS is built after that several tests (using NSL-KDD dataset) are carried out to show the detection capabilities.

The results showed IDS was able to distinguish between normal and abnormal packets, with an accuracy of (99.789%).In the online stage, the IDS is integrated with honeypot to check packets from the network. The result of testing the proposed system (online IDS with honeypot trap) show the ability to recognized and direct traffics either to honeypot trap (malicious traffics) or to the original destination (normal traffics).

Table of Figures

List of Tables

Table of Algorithms

List of Abbreviations

A	***Accuracy***
ACK	*Acknowledge*
AIDS	*Anomaly Intrusion Detection System*
API	*Application Programming Interface*
APT	*Advanced Persistent Threats*
ARPD	*Address Resolution Protocol Daemon*
DARPA	*Defense Advance Research Project Agency*
DB	*Database*
DLL	*Dynamic Link Library*
DNS	*Domain Name System*
DOS	*Denial of Service*
DR	*Detection Rate*
DT	*Decision Tree*
FN	*False Negative*
FP	*False Positive*
FTP	*File Transfer Protocol*
GR	*Gain Ratio*
GUI	*Graphics User Interface*
HIDS	*Host-Based Intrusion Detection System*
HTML	Hypertext Markup Language
HTTP	*Hypertext Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IGMP	*Internet Group Message Protocol*
IIS	*Internet Information Service*
IP	*Internet Protocol*
IPv4	*Internet Protocol version 4*
ISP	*Internet Service Provider*
KDD	*Knowledge Discovery in Database*

LAN	*Local Area Network*
MIT	*Massachusetts Institute Of Technology*
NAT	*Network Address Translation*
NIC	*Network Interface Card*
NIDS	*Network Intrusion Detection System*
NSL	*Network Socket Layer*
OSSEC	*Open Source Security*
PCAP	*Packet Capture*
R2L	*Remote To Local*
SIDS	*Signature Intrusion Detection System*
SOM	*Self-Organizing Map*
SPAN	*Switched Port Analyzer*
TCP	*Transmission Control Protocol*
TF	*Term Frequency*
TN	*True Negative*
TP	*True Positive*
UC	*Unsupervised Clustering*
UDP	*User Datagram Protocol*
U2R	*User To Root*
VC#.NT	*Visual C Sharp Dot Net*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

Content

Chapter Three Design of the Proposed System page

Chapter Four Implementation, Results and Discussion

page

Chapter five Conclusions and Suggestions for Future Work *page*

Chapter One

Introduction

1.1 Overview

The advancement of internet technology and computers helps to increase the spread of internet services to many different places, where the use of computers and internet service became available at home or business. Because of this continuous development, security loopholes have increased significantly, so it is necessary to develop methods and tools for preventing attacks that usually target vulnerable systems. The objective of security includes protection of computers, networks, software, information, and property from theft, corruption, or alteration while allowing the information and property to remain accessible and productive to its intended users [1]. Computer security is the protection that afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, telecommunications, information, and data). Network security consists of many policies dedicated by the network administrator to detect and prevent modification, misuse, or access to network resources [2].

Many security methods are used to provide protection, such as intrusion detection, the honeypot trap system, and a firewall. All these share the same goal of protecting and maintaining the services and information provided to users. Intrusion detection systems monitor and analyze data passing through the network. In case of abnormal data traffic, these systems launch a warning to the network administrator,

which in turn performs the necessary action by preventing unauthorized access and restricting the movement of data or other defensive means [3].

Honeypot systems are a technology used to trick attackers to attack them, thus record all the events and actions, and then store them for analysis. The main objective of the honeypot is to show the new methods and behavior of the attacker to take advantage of this information in the manufacture of a database for protection and defense systems [4].

1.2 Related Work

- In 2004, Christian Kreibich and Jon Crowcroft [5] present a work entitled "Honeycomb–Creating Intrusion Detection Signatures Using Honeypots", they used a system for automated generation of attack signature for network intrusion detection system. This system applies pattern-recognition techniques and protocol conformance check (they examine IP, TCP, UDP headers and payload data) to the network traffic captured by honeypots. They extended the open source free honeypot program called "Honeyd" by a subsystem that captures traffic inside the honeypot. The system generates a signature by analyzing traffic captured by extending Honeyd and supporting these signatures for Bro and Snort programs (Bro and Snort are open sources programs used for Network Intrusion Detection Systems (NIDS)).

- In 2005, Hassan Artail and Haidar Safa [6] present a work entitled "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks". They used Honeyd, Honeynets, and Snort for building a hybrid honeypot approach combine both the high and the low interaction honeypots in one framework to provide more information about intruder's behavior. The main idea was deployed low interaction honeypot Honeyd to emulate services, operating systems, and direct malicious traffic to high interaction honeypots (Honeynets), where intruder engages with the real operating system [5].

- In 2008, Babak Khosravifar and Jamal Bentahar [7] present a work entitled "An Experience Improving Intrusion Detection Systems False Alarm Ratio by Using Honeypot". They proposed an architecture composed of distributed agents and honeypot. In this system, alarming adversaries is initially detected by IDS (using Snort program), will be rerouted to honeypot (Honeyd) for more investigation. If the result of the investigation proved that the alarm caused by IDS is wrong, the connection will be forwarded to the original destination in order to continue the previous interaction. By using this scheme, the alarming rate with a decrease and the performance of IDS will be increased. They proposed the director (act as commander) for shifting the connection with all related data of the original destination to the honeypot.

- In 2008, Nirmal Dagdeeand and Urjita Thakar [8] present a work entitled "Intrusion Attack Pattern Analysis and Signature Extraction for Web Services Using Honeypot". They proposed an approach to analyze the attacks and generate signatures for web services. The proposed approach consists of three components; data logging, data analysis, and signature extraction. In data logging component, they used Honeyd and Tcpdump (Tcpdump is a program used for traffic analysis) for data collection. Data analysis component is responsible for analyzing data and extracting precise attack signature. Signature extraction component contains an extraction mechanism for good quality attack signatures.

- In 2009, Ram Kumar Singh and T. Ramanujam [9] present a work entitled " Intrusion Detection System Using Advanced Honeypots". They developed a system that combines IDS and honeypot for increasing the security and reliability of the network. This system attempts to load balance between network performance (throughput and latency) and tools for providing security (IDS and honeypot). The load balancer receives the incoming packet, opens TCP connection to IDS process, and sends the content of packet over that connection. IDS checks the packet and send a boolean result to load balancer. If the result were true, the load balancer would forward packets to the honeypot trap, otherwise, the load balancer would forward packets to the production system.

- In 2010, Yun Yang and Jia Mi [10] present a work entitled " Design and Implementation of Distributed Intrusion Detection System Based on Honeypot". They proposed a system making use of honeypot to collect the invasion characteristics on the network and use the method of unsupervised clustering (UC) and genetic clustering to extract the data for analysis. They combined anomaly detection (based on the protocol to capture unknown attacks) and signature detection (use the signature to match the pattern for known attack) for producing hybrid IDS. They used the honeypot trap to extract signature for unknown attack and store them in the intrusion database. Unsupervised clustering and genetic clustering are used for mining invasion features from the honeypot's audit record.

- In 2012, Liu Dongxia and Zhang Yongbo [11] present a work entitled" "An Intrusion Detection System Based on Honeypot Technology". They proposed an intrusion detection module using the mobile agent environment, this module has the capability to distribute detection and response. Mobile agent environment is the heart of the model structure of the entire system; it is responsible for control the entire system, control the production of the agent, cloning, log off, distribution and recycling. The proposed system traces the intrusion source farthest by means of honeypot technology. The use of honeypot technology to get the maximum extent of possible attack information in order to facilitate the further invasion of the source tracking, and signature data to achieve timely and automatic updates.

- In 2013, Roman Jasek and Martin Kolarik [12] present a work entitled "APT Detection System Using Honeypots". They proposed a practical solution to detect Advanced Persistent Threats (APTs). APT is precisely focused on specific targets; according to the knowledge of the environment and selection appropriate types of attacks, so that it differs from traditional forms of hacking. They initially focused on gathering information about the network configuration and server operating system, after that focus on setting up rootkits and other malware to interact with other attackers to steal intellectual property and financial gain. They extend the agent program to direct the attacker to honeypot for more details information.

- In 2015, Vishal Mehta and Pushpendra Bahadur[13] present a work entitled "Threat Prediction Using Honeypot and Machine Learning ". They tried to predict threat using a honeypot as a source of data and various machine learning algorithms. They used three open source program, which are OSSEC (Open Source Security program is a host-based intrusion detection system used to alerting and maintaining the integrity of data), Snort and honey.OSSEC program used as Host Intrusion Detection System (HIDS), Snort program for NIDS and Honeyd program as a honeypot.

- In 2016, Janardhan Reddy and Santosh Kumar [14] present a work entitled "Honeypot–Based Intrusion Detection System: A Performance Analysis ". They proposed a virtual honeynet architecture that implements virtual honeynet collaboration systems (VHCS). The system consists of Honeyd for creating low interaction honeypot, snort as an intrusion detection system and

ARPD (Address Resolution Protocol Daemon) program to monitor unused IP space and direct attacks to Honeyd.

- In 2017, Neha Agrawal1 and Shashikala Tapaswi [15] present a work entitled " The Performance Analysis of Honeypot Based Intrusion Detection System for Wireless Network ". They proposed a method named Honeypot Intrusion Detection System (Honeypot IDS) for the detection and prevention of Rogue Access Point via attack detection performed by internal and external malicious users. Honeypot IDS combines Intrusion Detection System and Honeypot, to reduce false alarm rate generated by existing IDS.

1.3 Problem Statements

The integration of the intrusion detection system with the honeypot system has recently shown great interest in protection and security. However, three problems should be considered in this research. The first problem is how to make IDS check malicious traffics with less false negative and false positive? The second one is how to take advantage of the honeypot in the network in which the intrusion detection operates? Finally how to analyze the data obtained from the honeypot to create the new pattern (signature) used in intrusion detection system?

1.4 Aim of Thesis

The aim of work is to design and develop an effective security system based on the principles of intrusion detection and deception concept (using honeypot system) to provide protection against intruders from outside or inside the network. The proposed intrusion detection system is based on signature or pattern to classify traffic either normal or abnormal.

The main objective of the honeypot trap is to take away the intruder from the production system to a fake system in order to get more information about the intruder. The proposed system integrates Intrusion detection system with deception tool (honeypot) to produce a powerful immunity system against intruders.

1.5 Thesis Contribution

The most important contribution can be summarized as follows:

- Create IDS engine using the C4.5 algorithm and deploy it in the network.
- A router using rules to block or forward traffic. The creation of rules done manually by an administrator. In this work, a new program designed for creating and adding the rules in a dynamic manner to the router without the intervention of an administrator.
- Configuring and deploying a physical honeypot trap with several servers (web, FTP (File Transfer Protocol), DNS (Domain Name System), telnet). The honeypot contains a number of open port assign to each server to attract more attackers.
- The proposed can be used to protect not only the network but also individual users because IDS can work with or without a honeypot trap.