International Journal of Computer Networks and Communications Security

VOL.2, NO.1, JANUARY 2014, 39–45
Available online at: www.ijcncs.org
ISSN 2308-9830

Monitoring and Analyzing System Activities Using High Interaction Honeypot

Dr.Najla B. Al-Dabagh[1] and Mohammed A. Fakhri[2]

[1, 2] Computer Science Dept. College of Computer Science and Mathematics, Mosul University, Mosul, Iraq

E-mail: [1]najladabagh@yahoo.com, [2]Mohammed_a_f@yahoo.com

ABSTRACT

Honeypot is one of protection techniques that have been used recently in the field of networks security, characterized by their effectiveness in detecting new attacks and interaction with the attackers and providing a suitable environment for them to do their attacks. After that studying the attacks, analyzing and be an impression of the attacks and the attackers. This is what distinguishes it from traditional intrusion detection systems. Still Denial of Service (DoS) attacks pose a major challenge in the online world to this day. DoS attacks characterized by many features such as easy to launch, and a large-scale, used by novices to the presence of tools based attacks .Therefore, most of the research's concerned with disclosure of denial of service attacks. In this work a high interaction honeypot is designed to detect Denial of Service attacks by analyzing packets and extracting their features, by applying one of decision tree algorithm (C4.5) to detect attacks. The proposed Honeypot monitors the system and analyzes events to detect unknown attacks by Open Source Security (OSSec).

Keywords: *Honeypot, DoS, Decision tree, OSSEC.*

1 INTRODUCTION

Today's world increasingly relies on computer networks. The use of network resources is growing and network infrastructures are gaining in size and complexity. This increase's followed by a rising volume of security problems. New threats and vulnerabilities are found every day, and computers are far from being secure. In the first half of 2013, 4,100 vulnerabilities were detected by vendors, researchers and independents [1].

The consequences of these vulnerabilities affect users and businesses dramatically in terms of the privacy issues and financial losses. One such technology that has gathered considerable attention from industry analysts and trade media is "honeypot" technology. Honeypots, considered by many as the hottest new intrusion protection technology, are used to contain and control an attack. They are used much like deception techniques in warfare that divert enemies into attacking false troops or airfields. These systems can be applied to defend networked assets from today's savvy attackers waging a new kind of war on the enterprise [2].

L. Spitzner defines the term honeypot as follows:

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource [3].This means that a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional and valuable information.

The Denial-of-Service (DoS) attack remains a challenging problem in the current Internet. In a DoS defense mechanism, a honeypot acts as a decoy within a pool of servers, whereby any packet received by the honeypot is most likely an attack packet. A denial-of-service (DoS) attack is an explicit attempt by attackers to prevent an information service's legitimate users from using that service. These attacks, attempt to exhaust the victim's resources, such as network bandwidth, computing power, or operating system data structures. Flood attack, Ping of Death attack, SYN attack, Teardrop attack, DDoS, and Smurf attack are the most common types of DoS attacks. The hackers who launch DDoS attacks typically target sites or services provided by high-profile

organizations, such as government agencies, banks, credit-card payment gateways, and even root name servers [4]. This paper gives an overview of honeypot technology and classification, propose a high interaction honeypot for windows environment to detect attacks using decision tree algorithm to judge whether the collected features is normal or attack. Monitoring file system and Registry using an open source Host based Intrusion Detection System (HIDS), Open Source Security (OSSec) that look directly at log files and system behavior to spot oddities such as successful brute force attacks or evidence of rootkit installation.

2 RELATED WORKS

J. Briffaut et al [5], presents the design of secured high-interaction honeypot and discusses the results. A clustered honeypot is proposed for two kinds of hosts. The first class prevents a system corruption and never has to be reinstalled. The second class assumes a system corruption but an easy reinstallation is available. Various off-the-shelf security tools are deployed to detect a corruption and to ease analysis. Moreover, host and network information enable a full analysis for complex scenario of attacks. The solution is totally based on open source software.

Vinu V Das [6], focused on freeze private services from unauthorized sources against address spoofing DDoS attacks. This is achieved by controling attack traffic to its source using the pushback mechanism, for tracing back to a particular source, and by the ability to defend the attackers using roaming honeypots.

Yang et al [7], proposed honeypot system based on the distributed intrusion tracking different from traditional honeypot system, uses distributed deployment for improving the entire system protection area, and has certain expansion ability. System identifies invading characteristics through the invasion of feature database, can be compatible with Snort feature library, and can identify latest invasion characteristics by the way of upgrading in real time.

Divyaet al [8], developed Intrusion detection system consists of a hybrid honeypot with genetic algorithm. Where used a low interaction honeypot to interact with known attacks. And high interaction honeypot to interact with the unknown attacks.

J. Wangetal [9], proposed an intrusion detection algorithm based on C4.5 decision tree. In the process of constructing intrusion rules, information gain ratio is used in place of information gain. The experiment results show that: The intrusion detection algorithm based on C4.5 decision tree is feasible and effective, and has a high accuracy rate. The experimental data comes from KDD CUP1999 data sets. It is a test set widely used in intrusion detection field.

J.Zhaiet al. [10], proposed a honeypot in a network inveiglement system under strict surveillance, which attract attacks by real or virtual network and services so as to analyze the blackhat's activityes during honeypot being attacked by hackers, delay and distract attacks in the Meantime. The honeypots are valuable for developing new IDS signatures, analyzing new attack tools, detecting new ways of hiding communications or Distributed Denial of Service (DDoS) tools.

3 THEORETICAL CONCEPTS

3.1 Honeypot

A honeypot is primarily an instrument for information gathering and learning. Its primary purpose is not to be an ambush for the blackhat community to catch them in action and to press charges against them. The focus lies on a silent collection of as much information as possible about their attack patterns, used programs, purpose of attack and the blackhat community itself. All this information is used to learn more about the blackhat proceedings and motives, as well as their technical knowledge and abilities. This is just a primary purpose of a honeypot [11].

Honeypots are hard to maintain and they need operators with good knowledge about operating systems and network security. In the right hands, a honeypot can be an effective tool for information gathering. In the wrong, inexperienced hands, a honeypot can become another infiltrated machine and an instrument for the blackhat community [12].

The goal of the honeypot is to lure the hackers or attacker and capture their activities. This information very useful to study the vulnerabilities of the system or to study latest techniques used by attackers etc. There are several types of honeypots, which can be grouped into four major categories as shown in figure (1)

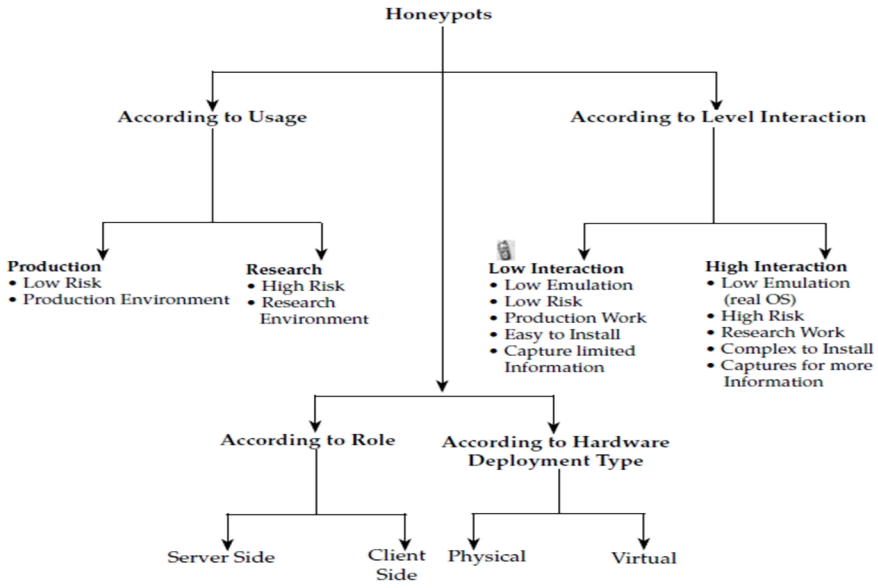

Fig. 1. Honeypots Classification [13]

3.1.1 Advantages

Honeypots have many advantages in network security include:

- Small Data Sets
- Minimal Resources
- Simplicity
- Discovery of new tools and tactics
- Reduce False Positive

3.1.2 Disadvantages

Honeypot disadvantages include:

- Limited Vision
- Discovery and Fingerprinting
- Risk of Takeover

3.2 Denial-of-Service (DoS) attacks

A particular troublesome type of attack on networked (computer) systems is the so-called Denial-of-Service (DoS) attack. The purpose of a DoS attack is to attack a system in such a way that the provided service is not more available or has become so poor that practical use of the service is no longer possible [14].Some of DoS attack that detected by proposed high interaction honeypot shown in table 1.

Table 1 : Some DoS attacks [15]

Attack Type	Attack description
ICMP flood	Sending a large amount of ICMP traffic to the victim machine to use up the network bandwidth.
Smurf	Floods the target machine with the spoofed broadcast ping messages. An attacker sends a large quantity of the ICMP echo request packets to many different network broadcast addresses; all packets have a spoofed IP address of the target victim.
UDP flood	Sending a large number of packets to the random ports on the target machine. The victim host will check for the application listening to a flooded port and most likely answer by an ICMP Destination unreachable packet.
SYN Flood	Sending the SYN requests to the target machine. The aim of the attack is to exhaust the allowed number of the half-opened connections. This prevents any new legitimate connections to be established.
LAND	Sending the spoofed TCP SYN packet with the victims target and destination addresses. As a result, the target machine will reply to itself continuously causing a lock up and denial of service

3.3 OSSec

OSSec is a scalable, multiplatform, open source (HIDS) Host-Based Intrusion Detection System. It has a powerful correlation and analysis engine, log analysis integration, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting, and active response. In addition to being deployed as an HIDS,it is commonly used strictly as a log analysis tool, monitoring and analyzing firewalls, IDSs,Web servers, and authentication logs. OSSEC runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris, and Microsoft Windows.OSSEC is free software and will remain so in the future. You can redistribute it and/ormodify it under the terms of the GNU General Public License (version 3) as published bythe Free Software Foundation (FSF). ISPs, universities, governments, and large corporate datacenters are using OSSEC as their main HIDS solution [16].

3.4 DecisionTree

DTs classifier by Quinlan [18] falls under the subfield of machine learning within the larger field ofartificial intelligence. The DT is a classifier expressed as a recursive partition of the instance space, consists of nodes that form a rooted tree, meaning it is a directed tree with a node called a root that has noincoming edges referred to as an internal or test node. All other nodes are called leaves (also known asterminal or decision nodes). In the DT, each internal node splits the instance space into two or more subspaces according to a certain discrete function of the input attribute values. In the simplest and most frequent case, each test considers a single attribute, such that the instance space is partitioned according to the attributes value [17].

C4.5 is an efficiency and popular learning type of the decision tree. Starts with large sets of cases belonging to known classes. The cases, described by any mixture of nominal and numeric properties, are scrutinized for patterns that allow the classes to be reliably discriminated. These patterns are then expressed as models, in the form of decision trees or sets of if-then rules, that can be used to classify new cases, with emphasis on making the models understandable as well as accurate [18].

4 THE PROPOSED HONEYPOT

In this paper, we have suggested a high interaction honeypot system for windows to detect attacks and monitoring the system. OSSSEC is used as HIDS to monitor the system and generate alert if any change happen in system registry and detect attack based on a collection of rules.Decision tree algorithm is used to classify data with common features. The proposed honeypot system consist of two major part that work simultaneously as shown in Figure 2.

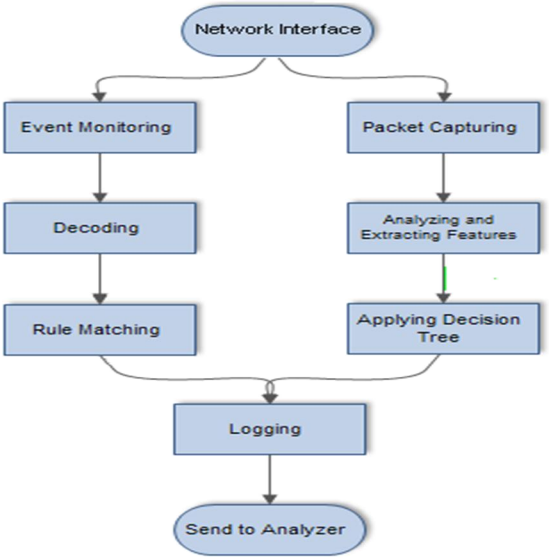

Fig. 2. Proposed Honeypot

4.1 Using OSSec as HIDS

OSSec is a host-based intrusion detection system. It configures to run on the Honeypot machine run scans and checks if anything relating to the machine's system has been changed. Any changes are recorded and an alert is sent off. This is useful because it helps us to see what effect any malicious activity has on the computer and so we can differentiate between traffic sources that have affected the system and those that haven't and what effect they have had on the system.

Event monitoring performs log analysis, file integrity checking, policy monitoring, rootkit detection. Decoding receive data from event monitoring and extract useful information (IP address information, usernames,URLs, and port information are some of the common fields that can be decoded from the event) for matching. Rule matching compare extracted data with OSSec rules to check if received event contain malicious activity .OSSEC stores all collecteddata into logs. This is the primary place where it is all stored. But this is not a very usefulformat and takes time to access it and find anything useful , therefore we using OSSec web user interface (OSSEC WUI) for better understand to alert that logged by OSSec.

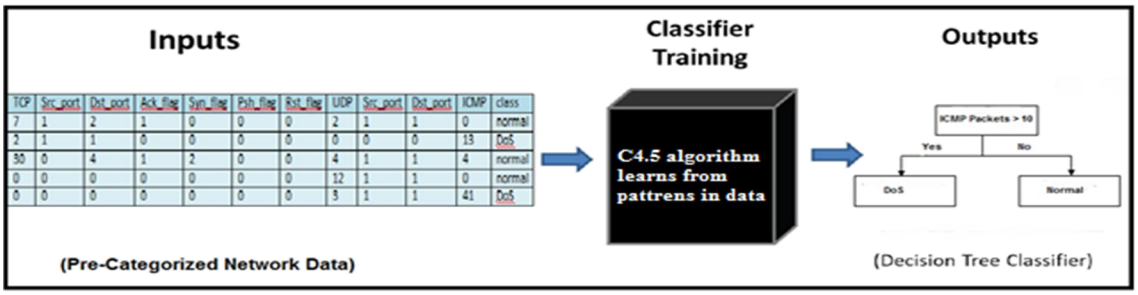

Fig. 3. Sample of Decision Tree training inputs and outputs

4.2 Detecting attacks using Decision Tree

Implementing decision trees can require some network data and tool, network data collected using raw socket that captured packets, extracting 11 features from each collected packets, separate these packets to records based on connection between two systems, using them to training decision tree with predefined class. Training process train decision tree with 13000 records using open source data mining analysis tool (Weka), Figure 4 show output tree for some of collected records.

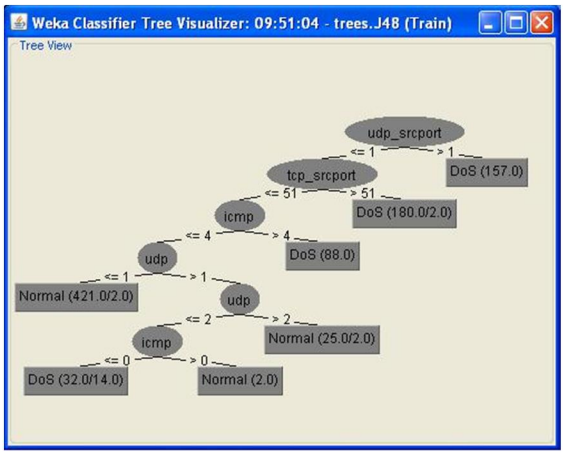

Fig. 4. Tree view for some records

Applying decision tree rule in real time using C# programming language in three steps:

1) Packet Capture: capture all incoming and outgoing packets.
2) Packet Analysis: analysis and extraction features, detect attacks.
3) Logging: log attack details and send it to the analyzer.

4.2.1 Packet Capturing

For capturing the packets, a raw socket is used in C# and bind it to the IP address. After setting the proper options for the socket, we then call the IOControl method is called on it. Notice that IOControl is analogous to the Winsock2WSAIoctl method. The IOControlCode.ReceiveAll implies that all incoming and outgoing packets on the particular interface be captured.The second parameter passed to IOControl with IOControlCode.ReceiveAll should be TRUE so an array byTrue is created and passed to it.

Algorithm to capture network packets

Step 1:Get list of all network interfaces and store them in Network_Interface[]

Step 2: Get each Network Interface name and its MAC addresses in the Network_Interface[]

Step 3: Choose Network_Interface to capture packets .

Step 4: Start capturing Packet using Raw Socket.

while start=enable

a. Print the Packets to Screen .

b. Send it to Packet Analysis

Step 5: End

4.2.2 Packets Analysis

This operation perform analysis of the captured packets and extracting information. These information including IP header, TCP header, UDP header, and ICMP header from each promiscuous packet. After that, the packet information is divided by considering connections between any two IP addresses (source IP and destination IP) and collect all records every 4 seconds .It is applied for each connection and classified it normal or attack.

Algorithm for packets Analysis

Step 1: Start capturing packets

- *For each packet pack*
  - *a) IF protocol=TCP*
  - *b) extract TCP features*
  - *else*
  - *c) IF protocol=UDP*
  - *d) extract UDP features*
  - *else*
- *e) IF protocol=ICMP*
- *f) extract ICMP features*

Step 2: Collecting features and wait 2 sec. .

Step 3: Separating the data into records by connection between 2 IP addresses.

Step 4: Apply decision treerules for each connection.

Step 5: Log result

Step 6: End

4.2.3 Logging

The log file contains information about attacker, date and time of attack and sends through periods of time to analyzer by Mail. OSSec logs attempts to access non-existent files Secure Shell attack, FTP scans, SQL injections, File System attack, Rootkit detection, Policy monitoring, and other host attacks based on signature rules.

5 EXPERIMENTAL RESULTS AND CONCLUSIONS

In this paper we proposed high-interaction honeypot that monitors and analyzes system to detect malicious activities and alert analyzer. Honeypot consists of two parts: first part to monitor system registry and policy and detect rootkits, using an open source tools .Second part to detect DoS flooding attacks by capturing raw packet extracting features and applying decision tree algorithm, then sending log file to analyzer.

To measure the effectiveness of a honeypot we used many tools that launch different DoS attacks from many computers (as shown in table 2). Proposed honeypot detected these attacks and generate alerts about them (as shown in figure 5).

Table 2: Some of attack tools.

Tools	Description
Net Tools	Launch HTTP, UDP Flooding
LOIC	Launch TCP,UDP,HTTP Flooding
B2 DoS	Launch UDP Flooding
BBHH-Ultra DoS	Launch SYN Flooding
ByteDOS v3.2	Launch SYN,ICMP Flooding
ServerDeath	Launch HTTP , UDP Flooding
iDoser v4	Launch UDP Flooding

Our experiments were carried out from launching attacks for two months on system, capturing packets, monitoring system activities and analyzing packets to decide which features was important and which data mining algorithm give best results. Trained training set with three algorithm decision tree C4.5 gives best result as shown in table 3.

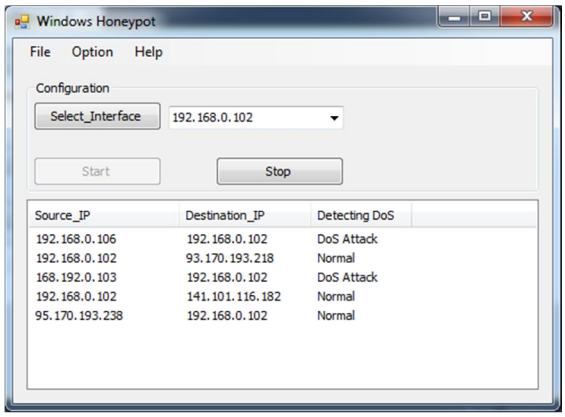

Fig. 5. System Interface

Table 3: Training data set with three algorithms

Features used	Classifier	Accuracy	Normal		DoS	
			TP	FP	TP	FP
11	C4.5	97.9537	0.999	0.004	0.959	0.001
11	OneR	86.2528	0.805	0.053	0.94	0.118
11	NaiveBayes	94.438	0.997	0.106	0.876	0.001

The honeypot is a new technology its aim to overcome traditional security tools. They are used together information of attacks and threats, its implementation in an organization will prove a useful security tool

6 REFERENCES

[1] IBM X-Force, 2013 Mid-Year Trend and Risk Report, CISO Security Insights, 2013.

[2] K.Meenakshi, M.NaliniSri, "PROTECTION METHOD AGAINST UNAUTHORISED ISSUES IN NETWORK HONEYPOTS ", International Journal of Computer Trends and Technology (IJCTT), volume4, Issue4, 2013.

[3] N.PROVOS, "A Virtual Honeypot Framework", In Proc. of 13th USENIX Security Symposium, 2004.

[4] A.Rama Mohan Reddy, K.Munivara Prasad, and V Jyothsna," IP Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, 2012.

[5] C. Toinard, J. Briffaut, and J.-F.Lalande, "Security and Results of a Large-ScaleHigh-

Interaction Honeypot ", JOURNAL OF COMPUTERS, VOL. 4, NO. 5,2009.

[6] Vinu V Das, " Honeypot Scheme for Distributed Denial-of-Service Attack", IEEE, 2009 ,

[7] 7- Yun Yang, Hongli Yang," Design of Distributed Honeypot System Based on Intrusion Tracking", IEEE, Communication Software and Networks (ICCSN), 2011, Pages: 196-198.

[8] Divya, AmitChugh," GHIDS: A HYBRID HONEYPOT SYSTEM USING GENETIC ALGORITHM", International Journal of Computer Technology & Applications, , Vol. 3 Issue 1, 2012, p187-191

[9] DasenRen, Juan Wang, and Qiren Yang, " An intrusion detection algorithm based on decision tree technology", IEEE, Asia-Pacific Conference on Information Processing , 2009,Pages: 333-335.

[10] Jiqiang Zhai, Keqi Wang, “Design and Implementation of Dynamic Virtual Network", IEEE, Proceedings of 2011 International Conference on Electronic&Mechanical Engineering and Information Technology, Volume: 4 Pages: 2131-2134, 2011.

[11] Narinder Kaur, "Honeypot", International Journal of Computing & Business Research,ISSN (Online): 2229-6166,2012

[12] AlokS hukla, Kanchan Hans, "Honeypots : Fighting Against Spam", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 1 Issue 3, May - 2012

[13] R.C. Joshi, Anjali Sardana, “Honeypots A New Paradigm to Information Security", Science Publishers, P.O. Box 699, Enfield, NH 03748, USA, 2011.

[14] Ben Smeets," (E)DoS Attacks", Project4 EDoS – Instructions, 2009.

[15] Denial-of-service attack - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Denial-of-service_attack.

[16] Andrew Hay, Rory Bray,and Daniel Cid" OSSEC Host-Based Intrusion Detection Guide", Elsevier Science,2008.

[17] Adnan Mohsin, Abdulazeez Brifcani, Adel SabryIssa, " Intrusion Detection and Attack Classifier Based on ThreeTechniques: A Comparative Study", Eng. & Tech. Journal, Vol.29, No.2, 2011.

[18] Quinlan J R,”C4.5 program for machine learning”, San Marteo Morgan Kaufmann Publisher, 1993.