Summarization of Honeypot- A Evolutionary Technology for Securing Data over Network, And Comparison with some Security Techniques

Snehal B Rase[1], Pranjali Deshmukh[2]

[1]Computer Science and Engineering, P.R.Pote College of Engineering Amravati, India

[2]Department of computer Science, P.R.Pote College of Engineering Amravati, India

Abstract: ***In the era of information and technology network security has become the core issue in every organizational network. There are many security mechanisms were used to provide the security to the network. This paper mainly focuses on honeypot mechanism. Honeypot is an exciting new technology with enormous potential for security communities. It is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. This paper is the summary of honeypot mechanism which is taken from 20+ research paper. Though the honeypot term is not new for us, there are many research has been done day by day to improve the security over network. In this paper the recent survey of honeypot mechanism over cloud by Alert logic 2014 has been included. This paper discusses about the concept of honeypot, history of honeypot, discusses about why company should have implement honeypot technology, application of honeypot. Furthermore Research paper includes the comparison between intrusion detection system and honeypot mechanism.***

Keywords: honeypot, IDS, firewall, security tools, network security.

1. Introduction

The number of people connecting to the Internet is increasing very rapidly. The ease of use and the connectivity the Internet provides is highly useful but the risks involved and malicious intrusions are also increasing day by day. Exploitation of computer networks is getting more common. It is completely critical for business organization as well as individuals to protect their data from serious threats that would aim to steal their information. There are many security solutions available in the market. Some of them are like Firewall, Intrusion Detection System (IDS), and Honeypot which are explained below. The traditional system security approach is slightly focused on defense but more attention has been drawn to aggressive forms of defense against potential attackers and intruders. The advanced decoy based technology called Honeypot is a similar form of protection against intrusion [7].

The idea of honeypots began in 1991 with two publications, “The Cuckoos Egg” and “An Evening with Breford”. “The Cuckoos Egg” by Clifford Stoll was about his experience catching a computer hacker that was in his corporation searching for secrets. The other publication, “An Evening with Berferd” by Bill Chewick is about a computer hacker’s moves through traps that he and his colleagues used to catch him. In both of these writings were the beginnings of what became honeypots [11]. Lance Spitzner, key member of a research group in the United States called Project Honeynet, defines the term honeypot as follows: “A honeypot is a resource whose value is in being attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable information.” A honeypot is a resource, which pretends to be a real target. The main goals are the distraction of an attacker and the gain of information about an attack and the attacker. Honeypots do not help directly in increasing a computer network’s security [3].

It is defined as a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other person’s computer systems. Honeypot is a trap; an electronic bait. It is a computer or network resources that appear to be a part of the network but have been deployed as sitting duck to entice hackers .We can define honeypot as an “information system resource whose value lies in unauthorized or illicit use of that resource.” Most honeypots are installed with firewalls. Honeypots and firewalls work in reverse direction to each other as the honeypots allow all traffic to come in but block all outgoing traffic. Most honeypots are installed inside network firewalls and is a means of monitoring and tracking hackers. Honeypots are a unique tool to learn about the tactics of hackers [14].

2. Literature Review

The first type of honeypot was released in 1997 called the Deceptive Toolkit. The point of this kit was to use deception to attack back [11].In 1998 the first commercial honeypot came out. This was called Cybercop Sting. In 2002 the honeypot could be shared and used all over the world. Since then honeypot technology has improved greatly and many honeypot users feel that his is only the beginning. In the year, 2005, The Philippine Honeypot Project was started to promote computer safety over in the Philippines.

This paper is the result of many research has been done previously. This paper Research in this area has resulted in a number of papers discussing specific topics concerning honeypots and how honeypots can be created and deployed [15]. There are number of techniques has been used for network security. The IDS can be defined as a tool [6] or software application that monitors the activities of the computer system and/or network due to the potential occurrence of malicious activities or breaches of security policy. The IDS produces reports for the control station. It is primarily focused on identifying and recording information about any events as well as reporting similar attempts [6].

The Simulating Networks with Honeyd is proposed in [17], in this paper Honeyd simulates virtual hosts on a network, and is actively used in Honeynet research today [16].

The Official Nmap Project Guide to Network Discovery and Security Scanning is proposed in [18], which says The Nmap Security Scanner is a free and open source utility used by millions of people for network discovery, administration, inventory, and security auditing.

Firewall provides the filtering and generates logs to further analyze any malicious activity or any violation policy of access control list, firewall rules [8]

There are several papers have been explored on the honeypot, to secure data over cloud in paper [19]. There is also paper on honeypot using artificial intelligence [3]. Some papers discusses about the concept of hybrid honeypot [4]. Some paper discusses about honeypot architecture in [20].

There is one survey has been done by alert logic in 2014 [21]. In early 2012, Alert Logic launched the first in a series of reports on cloud security, with the goal of creating the IT industry's first assessment of security in the cloud for businesses considering the use of cloud computing platforms.

3. The security techniques for networking

3.1 Intrusion Detection System

Intrusion detection systems introduced to overcome the shortcomings of existing network. Intrusion detection system silently monitor the network's traffic and give the alerts to tell about any kind of intruders based upon the database of signatures of existing intrusions. A number of issues were with IDS too as facing with an increasing number of false negatives and false positives. [1].

The IDS consists of several elements where the main element is a sensor, the mechanism for analysis, responsible for intrusion detection. This sensor contains a mechanism that makes decisions regarding a breach. The sensor receives data from three main sources of information: the IDS knowledge database, system logs and audit trails. System logs may include for example file system configuration and user permissions [6]. The layered-integrated model, as the name suggests is the combination of two IDS techniques namely integrated IDS and Layered IDS. This model was mainly proposed to solve two major concerns related to cloud computing, that are log management and high performance intrusion detection. The incoming data is first analyzed by risk assessment. After data is analyzed it becomes easy to distribute the data in different layers corresponding to their anomaly levels provided through risk assessment. This distribution is done within security core which implements feed forward artificial neural network which is capable of quick information processing, has self learning capabilities, and can tolerate small behavior deviations. Corresponding to their segregation the data is then passed to integrated model which implements one of the three analyses which can be behavior, knowledge or selected patterns. Once the user along with its data gets authenticated he is provided with requested services. [2]

Advantages of IDS

(a) IDS are easier to deploy as it does not affect existing systems or infrastructure.
(b) Network based IDS sensors can detect many attacks by checking the packet headers for any malicious attack like TCP SYN attack, fragmented packet attack etc.
(c) IDS monitor traffic on a real time. So, network based IDS can detect malicious activity as they occur.

Disadvantages of IDS

(a) IDS is not an alternative to strong user identification and authentication mechanism.
(b) IDS is not a solution to all security concerns.
(c) False positives occur when IDS incorrectly identifies normal activity as being malicious, False negatives occur when IDS fails to detect the malicious activity [8].

3.2 Firewall security

A firewall is a combination of hardware and software that isolates an organization's internal network from other networks, allowing some packets to pass and blocking others. It functions to avoid unauthorized or illegal sessions established to the devices in the network areas it protects. Firewalls are configured to protect against unauthenticated interactive logins from the outside world. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Basically, numbers of firewalls can be deployed in the proper positions of the managed network for cooperative, integrated, and in-depth network security protection. Administrators that manage the firewalls have a have to be careful while setting the firewall rules [8].

Advantages of Firewalls:

(a) Firewalls can prevent the traffic which is non-legitimate.
(b) A firewall helps protecting the internal network by hiding names of internal systems from the outside hosts.

Disadvantages of Firewalls:

(a) Firewalls use set of rules that are manually configured to differentiate legitimate traffic from non-legitimate traffic.
(b) Firewalls cannot prevent attacks coming from Intranet.

4. The idea of honeypots

A honeypot can be as simple as a single computer running a program to listen on any number of ports; when a connection is made, the program logs the source IP and alerts to owner with an e-mail. HONEYPOT resource has no REAL use. In other words, normal users will never connect to it. It is setup ONLY to lure the malicious users to attack it. Since, a HONEYPOT resource has no REAL use, and thus, if a system administrator notices a user connecting to it, then 99% of the times that user is a malicious one. The concept of Honeypots in general is to catch malicious network activity with a prepared machine. This computer is used as bait. A valuable compromised data is collected with the help of software that permanently collects data when a honeypot is attacked. [11], [14].

The two main reasons why honeypots are deployed are probe and attempt to gain access to your systems and gain insight into attack methodologies to better protect real production systems. Only within a properly configured network, one can assume that every packet sent to the Honeypot, is suspect for an attack. If misconfigured packets arrive, the amount of false alerts will rise and the value of the Honeypot drops. There are two categories of honeypots – production honeypots and research honeypots. A production honeypot is used to help mitigate risk in an organization while the second category, research, is meant to gather as much information as possible. These honeypots do not add any security value to an organization, but they can help to understand the blackhat community and their attacks as well as to build some better defenses against security threats [4]. A properly constructed honeypot is put on a network, which closely monitors the traffic to and from the honeypot. This data can be used for a variety of purposes [5].

First, honeypots do not solve a specific problem. Instead, they are a highly flexible tool that has many applications to security. They can be used everything from slowing down or stopping automated attacks, capturing new exploits to gathering intelligence on emerging threats or early warning and prediction. Second, honeypots come in many different shapes and sizes. They can be everything from a Windows program that emulates common services, such as the Windows honeypot KFSensor3, to entire networks of real computers to be attacked, such as Honeynet. In fact, honeypots don’t even have to be a computer, instead they can be a credit card number, Excel spread sheet, or login and password (commonly called honeytokens)[22]

Honeypots are classified based on its level of interactions. The word ‘interaction’ here means - the degree of communications that are being allowed for the attacker to exploit the honeypot [3].

(a) Low level interaction.

On the basis of interaction low interaction honeypots doesn’t provide Operating system access to the intruder .It provides only services such as ftp, http etc. These low interaction honeypots plays the role of passive IDS where the network traffic is not modified. Some examples of low interaction honeypots are honeyd, specter, BOF [3].

(b) Medium level interaction:

Like low interaction honeypots these also do not provide OS access to attacker but chances to be probed are more than low interaction honeypots .Some examples of medium interaction honeypots are Nepenthes.[3]

(c) High level interaction.

These are the most sophisticated honeypots .These are difficult to design and implementation .These honeypots are very time consuming to develop and have highest risks involved with this as they involve actual OS with them .In high Interaction Honeypots nothing is simulated or restricted. Some example of High interaction honeypots are Sebek, Argos [3]. In general every traffic from and to a honeypot is unauthorized activity. All the data that is collected by a honeypot is therefore interested data. Data collected by the honeypot is of high value, and can lead to better understanding and knowledge which in turn can help to increase overall network security. One can also argue that a honeypot can be used for prevention because it can detect attackers from attacking other systems by occupying them long enough and bind their resources [5].The table 1 shows some example of honeypot based on their interactions and purpose.

Table 1: Types of honeypot [1]

S No	Honepots	Types of honeypot	example
1	On the basis of interaction	low interaction	Honeyd, Kippo
		Medium interaction	Dionea, Napenthes
		High interaction	Specter
2	On the basis of purpose	Research honeypot	A standalone PC having any operating System installed like Linux.
		Production honeypot	kF sensor, specter,

5. Working of honeypot

The honeypot is a computer system running on the Internet which designed to lure and trick other people (such as hackers) who attempt to illegally break into others computer systems. Honeypot is mainly induced an attacker by using the network deception, makes the possible security vulnerabilities have very good camouflage place. Because honeypot cannot provide real value to the outside service, all of its attempt to link will be considered as suspicious. Another use of honeypots is to delay the attack on the real target, make the attacker waste time in a honeypot so that the possibility of a real network services to be detected is greatly reduced and the network detection rapidly detect the attempt of the invader. Afterward, timely repair security vulnerabilities that may exist in the system and receive the enemy's offensive skills and intentions. Honeypot tools include sensitive monitor and event log. Event log to detect an intruder to access and collect information on the activities and the same can be used as network evidences. Because any access to the honeypot system, the system is given the illusion of a successful invasion, so system administrators cannot expose the system really working conditions, timely shift, record, track intruders, to collect electronic evidence, do a better computer forensics work [23].

It is highly recommend deploying Snort with any honeypot deployment. Snort is an OpenSource IDS system that will not only detect and alert any attacks against your honeypot, but it can capture the packets and packet payloads involved in the attack. This information can prove critical in analyzing the attackers' activities [9], [10].

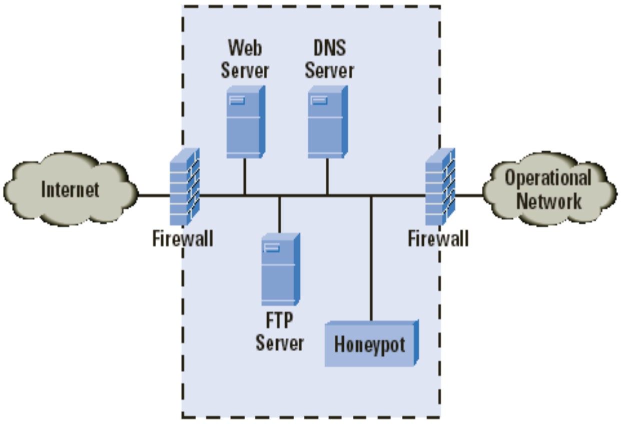

Figure 1: Working of a Honeypot [14].

For instance, honeypots often restrict outbound traffic in order to avoid attacking non-honeypot nodes. However, this restriction allows honeypots to be identified by an attacker. These redirection nodes also behave like real victims. Figure 2 shows the redirection of outbound traffic from a honeypot to another node in the honey farm.

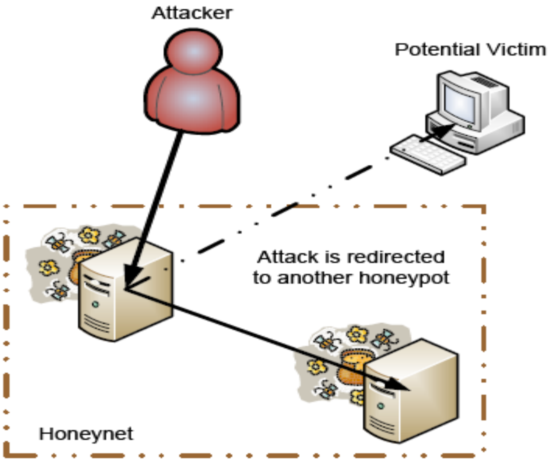

Figure 2: Redirecting an outbound attack in a Honeynet [6]

6. Comparison between IDS, firewall and Honeypot To Provide Security

6.1 Honey pots vs Firewalls

A firewall is designed to keep the attackers out of the network whereas honeypots are designed to entice the hackers to attack the system. This is done so that a security researcher can know how hackers operate and can know which systems and ports the hackers are most interested in. Also firewalls log activities and logs also contain events related to production systems. However in case of honeypot, the logs are only due to non-productive systems, these are the systems that no one should be interacting with. So a firewall log contains 1000 entries of all the systems of the network whereas the honeypots log only contain 5-10 entries [8]

6.2 Honeypots vs IDS

NIDS also suffer from high false positive rates. The value of a honeypot is determined by the information that can be obtained from it. Monitoring the data that enters and leaves a honeypot lets us gather information that is not available to NIDS. To detect malicious behavior, NIDS require signatures of known attacks and often fail to detect compromises that were unknown at the time it was deployed. On the other hand, honeypots can detect vulnerabilities that are not yet understood. Consequently, forensic analysis of data collected from honeypots is less likely to lead to false positives than data collected by NIDS.IDS is used as an alternative for building a shield around the network. The shielding approach is deficient in several ways, including failure to prevent attacks from insiders. IDS often depend upon signature matching or statistical models to identify attacks. This means that unknown or novel threats may not be detected. In contrast, honeypots are designed to capture all known and unknown attacks directed against them. Because any network activity related to the honeypot represents an anomaly, even the stealthiest activity will register on a honeypot [8].

7. Advantages of honeypots

Honeypots can capture attacks and give information about the attack type and if needed. New attacks can be seen and new security solutions can be created by looking at them. More examinations can be obtained by looking at the type of the malicious behaviors. It helps to understand more attacks that may happen. Honeypots are not bulky in terms of capturing data. They are only dealing with the incoming malicious traffic. Therefore, the information that has been caught is not as much as the whole traffic. Focusing only on the malicious traffic makes the investigation far easier. Therefore, this makes honeypots very useful. For the only malicious traffic, there is no need for huge data storage. There is no need for new technology to maintain. Any computer can be used as a honeypot system. Thus, it does not cost additional budget to create such a system. They are simple to understand, to configure and to install. They do not have complex algorithms. There is no need for updating or changing some things. As honeypots can capture anything malicious, it can also capture new tools for detecting attacks too. It gives more ideas and deepness of the subject proving that it is possible to discover different point of views and apply them for our security solutions [25]

8. Disadvantages of honeypots

We can only capture data when the hacker is attacking the system actively. If he does not attack the system, it is not possible to catch information. If there is an attack occuring in another system, our honeypot will not be able to identify it. So, attacks not towards our honeypot system may damage other systems and cause big problems. There is fingerprinting disadvantage of honeypots. It is easy for an experienced hacker to understand if he is attacking a honeypot system or a real system. Fingerprinting allows us to distinguish between these two. It is a not a wanted result of our experiment. The honeypot may be used as a zombie to reach other systems and compromise them. This can be very dangerous [25]. Implementing this system on an existing website could cause legality issues. Hence we intend to make dummy websites to demonstrate how our application functions. [5].

9. Application

(a) Honeypot can be used in Cyber Crime Investigation and Network Forensic System .
(b) Honeypot security system is using for e-banking
(c) Honeypot is used to Prevent DDos Attacks in Cloud.
(d) It is used in cloud computing to prevent data to be stolen by intruder.

10. Conclusion

Global communication is getting more important every day. At the same time, computer crimes are increasing. Countermeasures are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns. By knowing attack strategies countermeasures can be improved and vulnerabilities can be fixed. Honeypot comes into play for such purposes. It is a resource, which is intended to be attacked and computerized to gain more information about the attacker, and used tools.

Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. The traditional approach to security has been largely defensive so far, but interest is increasingly being paid to more aggressive forms of defense. One of these forms is decoy-based intrusion protection through the use of honeypots.

References

[1] Navneet Kambow et al, Honeypots: The Need of Network Security., (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101
[2] Swapnil Shinde1, Ashwini Bangar2, Manali Tawde3, Comparative Study and Analysis of Ids Implementation In Cloud Computing Environment, IOSR Journal of Computer Science (IOSR-JCE) e ISSN: 2278-0661, p-ISSN: 2278-8727 PP 33-39, 2014.
[3] A Review on Artificial Intelligence Techniques for Developing Intelligent Honeypot,International Journal of Advanced Research in Computer Science Engineering and Information Technology Volume: 3 Issue: 1 27-Jun-2014.
[4] K suresh, kush kumar yadav,r.srijit, karthik.p.bhat,hybrid honeypot -system for preserving privacy in networks, international journal of advanced research in computer science engineering and information technology, volume: 3 issue: 1 27-jun-2014,issn_no: 2321-3337.
[5] Juhi danani,jinal jani, Honeypot- A Tool to Trap Website HackersTCSC, Mumbai, India Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887)17-18 December 2012, ICRTITCS – 2012.
[6] Peter Fanfara, Marek Dufala, Ján Radušovský, Autonomous Hybrid Honeypot as the Future of Distributed,Computer Systems Security, Acta Polytechnica Hungarica, Vol. 10, No. 6, 2013.
[7] Narinder Kaur, Honeypot, International Journal of Computing & Business Research ISSN (Online): 2229-6166 Proceedings of ‘I-Society 2012.
[8] Tejvir Kaur1, Vimmi Malhotra2, Dr. Dheerendra Singh3, Comparison of network security tools- Firewall, Intrusion Detection System and Honeypot.nternational Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463 Vol. 3 Issue 2, February-2014.
[9] http://www.rbaumann.net.
[10] Http://www.christianplattner.net,
[11] Http://www.honeynet.org.
[12] Www.top site .com/best/ honeypot.
[13] www.en.wikipedia.org/Honeypot.
[14] *kemburu.*,.Honey-Pots , 53599210-14
[15] Karthik, S., Samudrala, B. And Yang, A.T. “Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 20 (4).
[16] Miss.Swapnali Sundar Sadamate, Review Paper on Honeypot Mechanism – the Autonomous Hybrid Solution for Enhancing International Journal of Advanced Research in Computer Science and Software Engineering Research Volume 4, Issue 1, January 2014
[17] R. Chandran, S. Pakala, “Simulating Network with Honeyd,”[online], Technical Paper Hybrid Solution for Enhancing., Paladion Networks, December2003.
[18] F. G. Lyon, “Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning,” [online], Nmap Project, USA, ISBN 978-0979958717, January 2009. Available on: http://nmap.org/book.
[19] Nithin Chandra S.R, Madhuri T.M , Cloud Security using Honeypot Systems , International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012, http://www.ijser.org .
[20] Ashwini pawar,kimaya Siddabhati, sadhana bhise, Snehaltamhne ,Web Application Honeypot. International Journal of Advance Research in Computer Science and Management Studies Research,Volume 2, Issue 3, March 2014 Article / Paper / Case Study Available online at: www.ijarcsms.com
[21] Alert logic cloud security report spring 2014, Https://www.google.co.in/?Gfe_rd=cr&ei=mqrrvixoesh 7vqt p84gaaq#q=alert+logic+cloud+security+report.
[22] Bhumika, Vivek Sharma Use of Honeypots to Increase Awareness regarding Network Security International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-2, June 2012,.
[23] Rajni mishra, Dr. renu dhir, Cyber Crime Investigation and Network Forensic System Using Honeypot. International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 1 Issue 4 November 2012 .
[24] Fabien Thalgott Honeypots in Network Security -29 Network Security 2DV00E, Linnaeus university, degree project

Author Profile

Snehal .B. Rase, received her B.E degree in 2010 from Amravti university. She was working as lecturer in Rambhau Lingade polytechnic college, Buldana during year 2010-2013, She is currently enrolled in M.E 1st year (2014-15).

Mrs. Pranjali Deshmukh, received her M.E degree from Amravati University, Currently she is working at P.R Pote college of Engineering, Amravati as Head of the Computer Science Department.