International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 6
ISSN: 2454-4248
63 – 65

Application of Honeypot in Cloud Security: A Review

Sushant Manchekar
Student, MCA Dept., L.B.H.S.S.T's, Bandra E
Mumbai University
Mumbai, India
sshntmnchkr@gmail.com

Makarand Kadam
Student, MCA Dept., L.B.H.S.S.T's, Bandra E
Mumbai University
Mumbai, India
macc.kd123@gmail.com

Krantee Jamdaade
Asst. Professor, MCA Dept., L.B.H.S.S.T's ICA, Bandra E
Mumbai University
Mumbai, India
krantee.jamdaade@gmail.com

***Abstract*—** In this paper, researcher is emphasizing on security handling in cloud computing using Honeypot. Now a days companies are providing cloud services for managing resources at higher level. Security Hurdle is a major issue in cloud computing that can be solved by implementing honeypot in cloud computing.

Keywords-*honeypot; cloud computing; cloud security; cloud*

*****

I. INTRODUCTION

A. *Cloud Computing*

Now days most of companies offer cloud computing because it is an emerging technology that helps business to improve service delivery capabilities. India has many cloud computing companies, which provide qualities in Private, Public and Hybrid cloud hosting.

B. *Cloud Security*

The interruptions over internet are cannot be completely removed but can be reduced. However computer crimes, data theft, lack internet security are increased in IT. IT security is works on three terms prevention, detection and respond. And honeypots are works on detection and respond category. In cloud computing their services has to be secure and protect their data of customers from hackers and unwanted access. [2]

C. *Honeypot*

Honey pot is certain computer system which is used for track and trapping hackers or uncertain users in cloud security system. Honeypots are designed for unconventional users, hackers for unkind and harmful activities over internet. [6] Honeypots are having two types. First one is Production honeypot are simple for deploy and it use to record few particular details. These honeypots are store into the production server for corporation safety reasons. This kind of honeypots are stored not as much data about cyber thief or criminals. Second one is Research honeypots are set for collect data about activities movement of Black Hat hackers; who focused on discrete network. Corporation use it for alert to secure the important data from attackers or hackers. These honeypots are multiplex to establish and conserve.

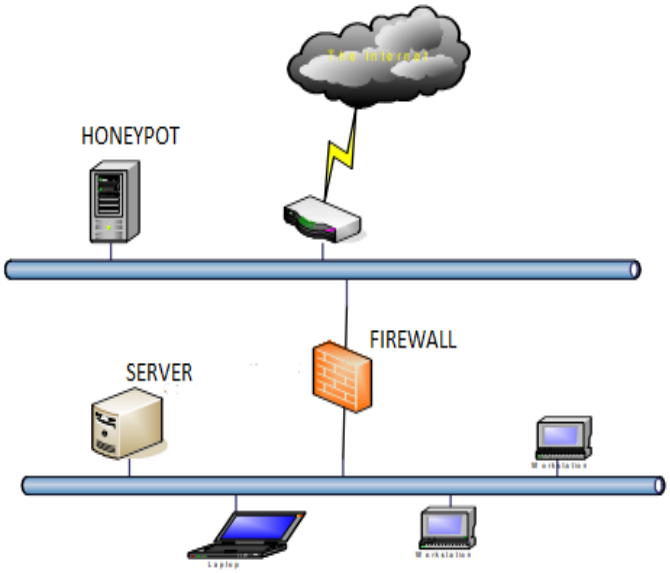

Figure 1.1 Architecture of Honeypots
Source adapted from [8]

According to the figure, architecture of honeypot designed into three layers. The purpose of the firewall is to filter the incoming traffic on a network. Honeypot host consist of honeypot service and host intrusion detection system (HIDS). This detection mechanism attracts worms to detect attacker, attacker details like IP addresses and method of attack. Process ID Tracking (PID) helps to identify unique process identification number in HIDS mechanism on a server.

II. LITERATURE REVIEW:

The Nithin Chandra S. R discussed about levels of honeypots according to their shape and size i.e. high interaction, Low interaction [2]. The Honeyd working is shown in figure 2.1(a),

ISSN: 2454-4248
63 – 65

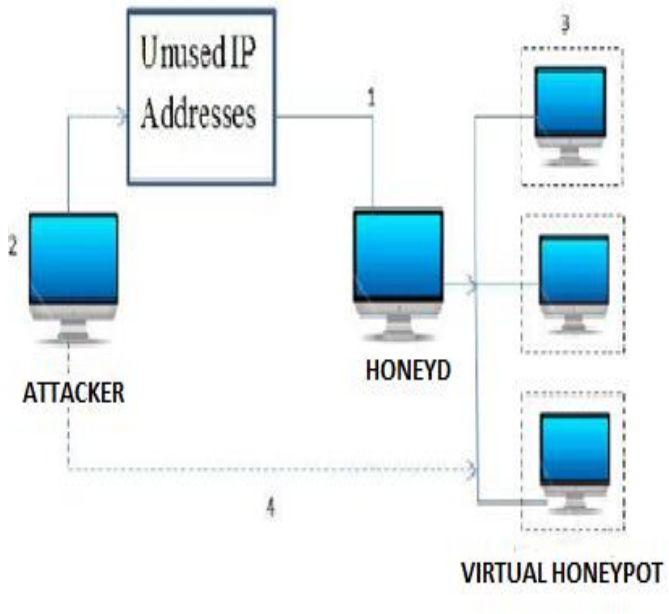

Figure 2.1(a) Honeyd Working
Source adapted from [2]

According to figure, the low interaction honeyd works on concept of monitoring unused IP space. When the attacker tries to attack get unused IP honeyd detect the IP and it creates virtual honeypot to fool attacker.

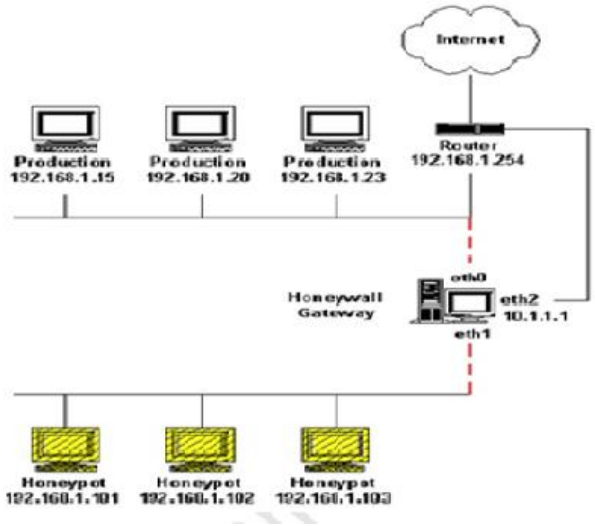

Figure 2.1(b) a honeynet
Source adapted from [3]

According to figure, the architecture of an entire network is designed to create a highly controlled network and honeynets do this using a Honeywall gateway.

According to Biedermann the cloning process of virtual machine where dynamic extraction has been done. The attacks can be delay with the help of VM cloning and monitoring of the deployed honeypot [3]. The group of authors proposing a new concept of fog computing this technology is used to launch disinformation attacks against malicious insiders to preventing real customer sensitive data [5]

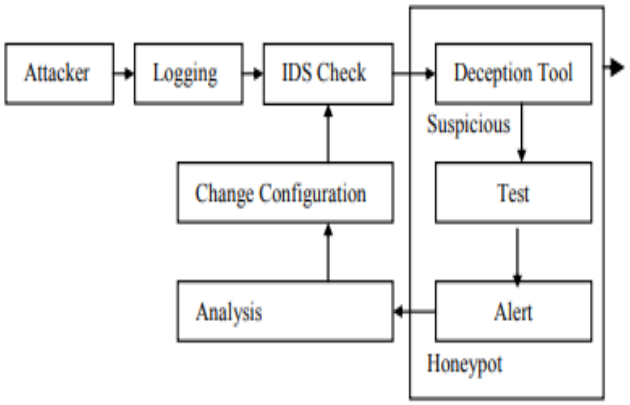

Figure 2.1(c) Honeypot Framework
Source adapted from [1]

Mahmoud T. Qassrawi says that in Honeypot framework deception plays a key role in honeypot success. Honeypots can use more effectively if it will use with security tools like Intrusion detection system (IDS) or Firewall. Honeypot also can be used to implement network security tools configuration ex. IDS or Anti-warm tools [8].

III. METHODOLOGY

A Stephen Brown ET. A focused-on Amazon EC2 and windows Azure cloud providers using some tools. p0f is a versatile OS fingerprint tool logs we used to gather some information about attacker and system he is using and used network as well as Analyzer setup is used to analyze the data generated across various honeypot instances. Backend and frontend infrastructures are designed for it. [4] Honeynet Security Console (HSC), Honeysnap, Bait-n-Switch etc. these tools extend the functionality of honeypots. [7]

The todays need of collecting attack details on large IP spaces are forced researchers to invent more scalable and intelligent architecture of honeypot is Hybrid honeypot and every virtual machine resource for each IP addresses is the methodology used according to Karthikeyan R. ET. A. [8]

Honeypots use deception to slow down attacks and detect new threat to modify network configuration as well as investigate the attacker. Deception is the basic idea of honeypot development it has some techniques as follows;

a) Deception service: works on request respond technique which listen on an IP service port and respond to network requests.

b) Operating system emulation: Honeypots can be deployed using virtual machine which match complete operating system ex.vmware,UML.

c) Operating system emulation: Instead of match operating system it emulates required parts of service.

d) Connection tarpitting: This technique will delay all type of network connections which helps to defend against computer worms attacks.[1]

 ISSN: 2454-4248
63 – 65

IV. RESEARCH FINDING:

Now a day's, the cloud security system mostly uses in private sectors for secure data from internal or external attackers. The organization are store private or confidential information on cloud. Cloud security system help to secure data from attacker or intruder by monitoring activity of attacker, IP Address, attacker detail using Honeypot or Honeynet system.

This kind of system required in India to prevent from Cyber Attack. In India Government sector store Public details like ADHAR, PAN, PASSPORT, etc. as well as Universities of India store important student data like admission detail, results, ERP on cloud. This data is large in size that's the reason Indian government need more security in cloud system to monitor attacker and delay attack to trap attacker. Honeypot is beneficial option for Indian cloud security.

V. CONCLUSION:

In our study we determine types of Honeypot with their different level of working in cloud security to detect attack and gather attacker details. In cloud computing the various architecture of honeypot and its different shape and size helps to protect sensitive data of customer. We observed that top companies like amazoneEC2, Azure, TCS (India) are using honeypots in cloud computing as well as startups and new companies also might be required honeypots in cloud computing for better services. Deception techniques are used to deploy honeypot and it be will largely use in future.

REFERENCES

[1] "Deception Methodology in Virtual Honypot", by Mahmoud T. Qassrawi, Zhang Hongli in IEEE © 2010.

[2] "Cloud Security using Honeypot Systems", by Nithin Chandra S.R, Madhuri T.M in IJSER © 2012.

[3] "Fast Dynamic Extracted Honeypots in Cloud Computing", by Sebastian Biedermann, Martin Mink, Stefan Katzenbeisser in ACM 2012.

[4] "Honeypots in the Cloud", by Stephen Brown, Rebecca Lam, Shishir Prasad, Sivasubramanian Ramasubramanian, and Josh Slauson in University of Wisconsin – Madison December 19, 2012.

[5] "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", by Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis in IEEE. 2012.19.

[6] "An overview of insider attacks in cloud computing", by Adrian Duncan, Sadie Creese and Michael Goldsmith in Wiley Online Library, 2014.

[7] "An Open-Source Honeynet System to Study SystemBanner Message Effects on Hackers", by Mark Stockman, Robert Heile, Anthony Rein in ACM. September 30–October 3.

[8] "Advanced Honey pot Architecture for Network Threats Quantification", by Karthikeyan R, Dr.T.Geetha, Shyamamol K.S, Sivagami G in International Journal of Engineering and Techniques 3, 2017.