TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The Cloud computing is a technique to store, share and access data anytime and anywhere with a device that is connected to a network, preferably the internet. Cloud computing consists of an expandable storage space with no physical storage space which is accessible from anywhere in the world using any device, by connecting it to the internet It contains large number of computing devices connected through a real-time communication (the internet) and has a common data storage area. The term “the cloud” is used as a metaphor for the Internet, based on the fact that a cloud like shape was used to indicate network telephone schematics, and later the Internet as an abstraction of underlying infrastructure it represents.

Honeypots are viewed as a successful technique to track programmer conduct and uplift the viability of security instruments. Honeypots are specifically designed to not only purposely engage and deceive hackers but also identify malicious activities performed over the Internet and can be counted as an effective method to track hacker behavior. Honeypots can be defined as systems or assets which is not only used to trap, monitor but also used to identify erroneous requests present within a network. They vary in the interaction provided to the attackers, from low interaction to medium and high, each type has its advantages and disadvantages. The aim is to analyze, understand, watch and track attacker’s behavior in order to create systems that are not only secure but can also handle such traffic. It is a closely monitored computing resource that we want to be probed, attacked, or compromised. More precisely, it is an information system resource whose value lies in unauthorized or illicit use of that resource.

.

1.1 PROBLEM STATEMENT

Cloud-based Honeypots give the capacity to explore and examine assaults that hit ordinary customers. Having them permits a specialist to interpret the IP locations and malware being utilized into security content that can ensure a normal cloud environment. Once those IP addresses have been distinguished, they will then lead a ping scope and defenseless output to discover a shortcoming in the system outline or vulnerabilities in programming that can be misused. It's conspicuous yet genuine; awful folks pursue the weakest focuses the most often. There are upsides of utilizing a cloud construct Honeypot in light of a cloud framework is like customary Honeypots in that it ought to have the capacity to decide whether a cloud framework has been traded off or endeavors were made to do so.

At last, they can essentially sit and log all movement coming into the cloud site in light of the fact that it's utilized for this particular reason practically any action ought to be dealt as instantly suspicious. Honeypots can serve to make dangers more obvious and go about as an early alert framework, which gives a cloud organization a more proactive way to deal with security instead of responsive. Any association with either outside resources/areas or cloud administrations ought to deploy cloud-based Honeypots.

1.2 MOTIVATION

First of all, we are very interested in this subject field of study. So, our motivation for this thesis is to understand how security systems are working and how an organization can be protected and being aware of the risks of security flaws in the system. We will learn how a system is working and how it can be developed. Once we have the results, we will examine the output with forensic science tools. While trying all these, we will come across some problems and we will try to solve it. At the same time we will have experience on creating and managing this kind of systems for the future. If we see similar problems in a network, we will be able to handle the system and recover the loss. Therefore, we will have a knowledge including both security problems examining and forensic science information gathering.

1.3 GOALS

We will find answers to all the questions that does the hacker know that it is a trap system? If the hacker realizes that it is a trap system does he continue attacking to it? What does he gain from attacking it? Our perspective is to solve the problems related to security, how a honeypot can be deployed, and the amount of information that we can get. We will look into the honeypot implementation and how far a network security administrator can go to obtain information and track the hackers. While looking for answers for security problems.

CHAPTER 2

LITERATURE REVIEW

2.1 CLOUD TECHNOLOGY

The Cloud Layers of Cloud Like an onion, the Cloud has many layers. It is usually divided into 3 layers:

Infrastructure as a service.

Platform as a service

Software as a service

Out of the three layers, SaaS is the top layer functioning off of both Paas and Iaas whereas IaaS is the foundation of the whole structure. The Infrastructure as a Service (IaaS) layer is physical hardware and therefore Honeypot deals with this layer. The Cloud is based on physical hardware suitable for computing (eg. nodes, servers, blades etc). Data are stored in what are called data centers (also known as DC) which are operated by web hosting professionals or network engineers.

Types of Security Threats

Cloud computing faces many security threats. These threats are of various forms. Following are the threats recognized at universal level:

1. Traffic Hijacking.
2. Insecure Interface and APIs.
3. Denial of Service.
4. Malicious Insiders.

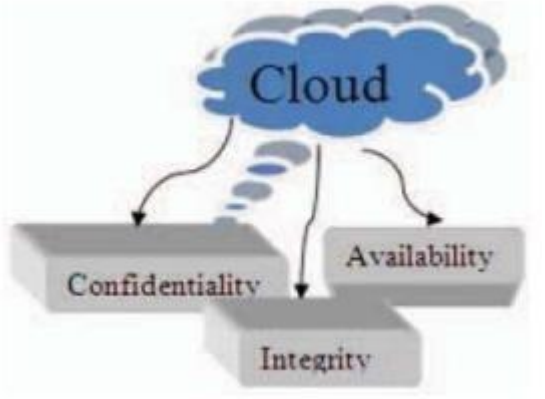

FIGURE2.1: SECURITY TRAID

2.2 HONEYPOT IN CLOUD

A Honeypot is a detection and security device which is required to be tested, assaulted, or bargained. The sole objective is to let the Honeypot be considered like any other normal machine or system by an unauthorized entity, presenting it as a bait. Their activity can be traced without being suspected when doing so. It is used to identify and react, instead of taking counteractive action, an area where it does not carry much expertise. Since Honeypots can't keep a specific interruption or spread of infection or worm, it just gathers data and identifies assault designs.

A Honeypot is a device to gather confirmation or data, and to pick up however much learning as could reasonably be expected particularly on the assault designs, hacker's reason and inspirations and the normally utilized projects propelled by them. From all the data, we can know more about the hacker's capacity particularly their specialized learning. Honeypots can be utilized to divert malicious programmers from general frameworks to the Honeypot framework. It can be implemented in a cloud-based environment by either placing it before the firewall or after the firewall. Another way is to implement it through an application which not only provides detection but also provides security to the files being shared through that application. This App can later be uploaded/deployed on a server which can also act as a cloud later. A cloud system with Honeypot present at its base is far more protected than the ones that do not contain it.

CHAPTER 3

HONEYPOT TECHNOLOGY

3.1 HISTORY OF HONEYPOT

In this part, we will give the history of honeypots so far according to LanceSpitzner.

1990-1991: It is the first time that honeypot studies released by Clifford Stoll (The Cuckoo's Egg) and Bill Cheswick (An Evening With Berferd).

1997: Deception Toolkit version 0.1 was introducted by Fred Cohen. After Clifford Stoll (The Cuckoo's Egg) and Bill Cheswick (An Evening With Berferd), Deception Toolkit gave an idea of first honeypot structure.

1998: First commercial honeypot was released which is known as CyberCop Sting.

1998: BackOfficer Friendly honeypot was introduced. It was free and easy to configure. It is working under Windows operating system. Most of the people tried this software and the concept of honeypot became more and more known among people.

1999: After BackOfficer Friendly, people were more into this new technology. Honeynet project started at this year. Also, Know Your Enemy papers were also released. Thanks to these releases, people understood the aim of the honeypots more.

2000-2001: Honeypots started to be used for capturing malicious software from internet and being aware of new threats. Companies began to use honeypots in their systems to improve security and see the malicious traffic.

2002: Honeypot concept became popular and honeypots improved their functionalities, so they became more useful and interesting for both researchers and companies.

3.2 WORKING PRINCIPLE

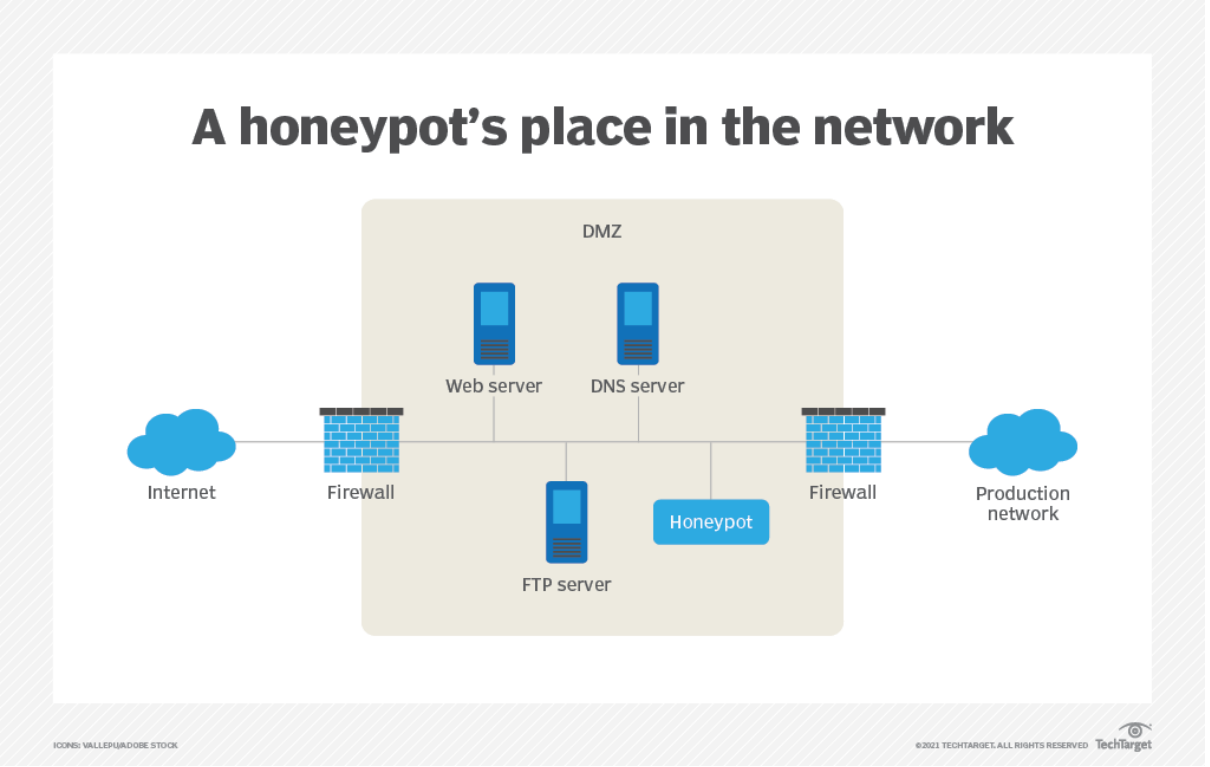

FIGURE 3: HONEYPOT WORKING PRINCIPLE

Cloud Generally, a honeypot operation consists of a computer, applications and data that simulate the behavior of a real system that would be attractive to attackers, such as financial system, internet of things (IoT) devices, or a public utility or transportation network. It appears as part of a network but is actually isolated and closely monitored. Because there is no reason for legitimate users to access a honeypot, any attempts to communicate with it are considered hostile.

Honeypots are often placed in a demilitarized zone (DMZ) on the network. That approach keeps it isolated from the main production network, while still being a part of it. In the DMZ, a honeypot can be monitored from a distance while attackers access it, minimizing the risk of the main network being breached.

Honeypots may also be put outside the external firewall, facing the internet, to detect attempts to enter the internal network. The exact placement of the honeypot varies depending on how elaborate it is, the traffic it aims to attract and how close it is to sensitive resources inside the corporate network.

No matter the placement, it will always have some degree of isolation from the production environment.

Viewing and logging activity in the honeypot provides insight into the level and types of threats a network infrastructure faces while distracting attackers from assets of real value. Cybercriminals can hijack honeypots and use them against the organization deploying them. Cybercriminals have also been known to use honeypots to gather intelligence about researchers or organizations, act as decoys and spread misinformation. No matter the placement, it will always have some degree of isolation from the production environment.

3.3 CLASSIFIACTION

Based on level of interaction Honeypots can be classified based on the level of interaction between intruder and system. These are Low interaction, high interaction and medium interaction honeypot

- Low-interaction honeypot: These types of honeypots have the limited extend of interaction with external system. FTP is the example of this type of honeypot. There is no operation system for attackers to interact with, but they implement targets to attract or detect attackers by using software to emulate features of a particular operating system and network services on a host operation system. Main advantage of this type of honeypot is that, it is very easy to deploy and maintain and it does not involve any complex architecture. With this advantage there is also some drawback of this system. That is, it will not respond accurately to exploits. This creates the limitation in ability to aid in discovering new vulnerabilities or new attack patterns. Low- interactive honeypots are a safer and easy way to gather info about the frequently occurred attacks and their sources.
- High-interaction honeypot: this is the most advanced honeypot. This type of honeypot have very higher level of interaction with the intrusive system. It gives more realistic experience to the attackers and gathers more information about intended attacks; this also involves very high risk of capturing of whole honeypot. High interaction honeypot are most complex and time consuming to design and manage. High interactive honeypots are more useful in the cases, where we want to capture the details of vulnerabilities or exploits that are not yet known to the outside world. This honeypots are best in the case of “0-Day attacks”
- Medium-interaction honeypot: these are also known as mixed-interactive honeypots. Medium-interaction honeypots are slightly more sophisticated than low-interaction honeypots, but are less sophisticated than high-interaction honeypots. It provides the attacker with a batter illusion of the operation system so that more complex attacks can be logged and analyzed. Ex: Honeytrap: it dynamically creates port listeners based on TCP connection attempts extracted from a network interface stream, which allows the handling of some unknown attacks.

Honeypots can be classified based on the purpose as Research honeypot and Production honeypot.

- Research honeypot: Research honeypots are basically used for learning new methods and tools of attacks. Research honeypots are used to gather intelligence on the general threats organizations may face, which gives the organization a better protection against those threats. Its main goal is to gain info about the way in which the attackers progress and performs lines of attacks. Research honeypots are complex to build, deploy and manage. They are basically used by organizations like universities, governments, the military and intelligence systems to learn more about threats. Research honeypots provides a strong platform to study cyber- threats and forensic skills.
- Production honeypot: production honeypots are simply aimed to protect the network. Production honeypots are easy to build and deploy, as they require very less functionalities. They protect the system by detecting attacks and giving alerts to administrators. It is typically used within an organization environment to protect the organization.

Based specialized technologies

- Spam honeypots**:** These can detect the methods of spammers, monitor their activity and block spam.
- Client honeypot: These actively seek out malicious servers behind client attacks instead of passively waiting for connections. They use virtualization to establish themselves on the server and watch for suspicious modifications to the honeypot.
- Database honeypots: These create decoy databases to mislead attackers using methods that are sometimes missed by firewalls, like Structured Query Language (SQL) injections.

CHAPTER 4

IMPLEMENTATION

4.1 METHODOLOGY

There are Various of ways in the vision of possibility when talking about an attack on the system in order to discover some faults and vulnerabilities of that same target system so that some kind of advantage can be taken out of it. Honeypot tends to perform as a surveillance tool and can also provide an early warning if required. It is a computer system or a site or an application that not only appears to be an isolated part of the network but usually also contains the information that is can be valuable attacking entity, which are highly trained to exploit the data to such an extent that it can harm the firm.

The new technique of protecting data and resources in a cloud through Honeypot by implementing it through an application on the infrastructure (Cloud Computing Environment). There are many restraints that need to be followed while implementing a Honeypot. The application makes it possible to store as well as share a document. While sharing or uploading the document it is encrypted using a password. If the correct password is not given then no message would be displayed rather the attacker would be shown an empty file. Since the actual working of a Honeypot involves silent detection, hence the application tracks the IP address of the user so that later the admin can review it and recognize the malicious entity

4.2 RESULT

Data sets are small as Honeypots collect the data about any malicious activity which includes attack or any kind of unauthorized act. Honeypots collect the data which can be easily managed and analyzed. False Alarms about a attack are reduced when they capture unauthorized activity. Honeypots usually tend to make use of least possible number of resources. Even encrypted attacks can be captured by Honeypots. Some versions of Honeypot are easily deployed and hence can be easily maintained.

Figure 4.1: LOGIN PAGE

The above figure shows the initial login page of the app, where the user can log into their account using their email address and password.

FIGURE 4.2: PERSONAL ACCOUNT DETAILS

After logging into the account, the user's details (name, contact number, email, and location) can be seen. Operations such as loading of file, receiving files, sending files and downloading files are done from this page as well, as shown in the above figure.

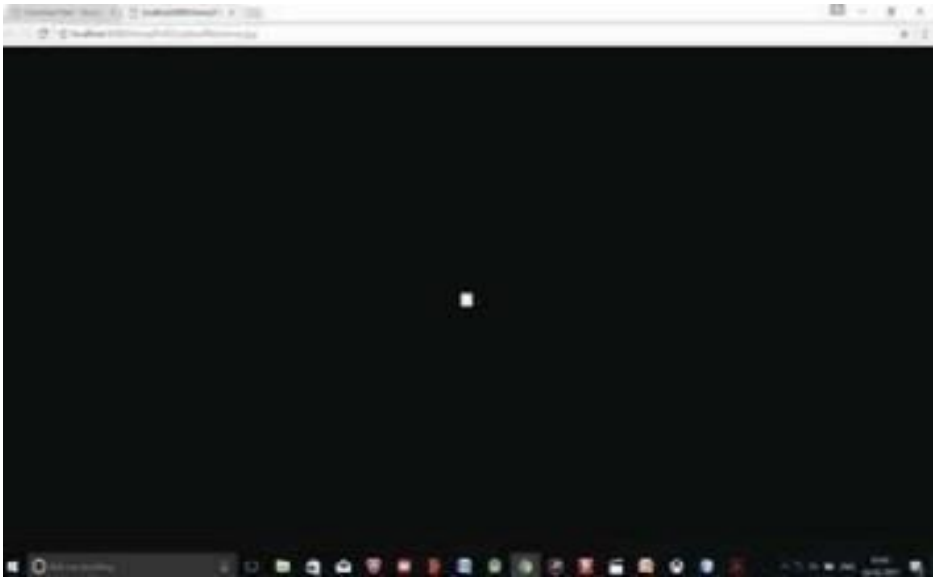

FIGURE 4.3: UNAUTHORSIED USER

The above figure shows a blank screen which contains an empty file. This is the page that will be visible to the unauthorized user if an intrusion takes place.

CHAPTER 5

ADVANTAGES

There are many security solutions available in the market. Anyone can browse the variety of choices through internet and find the most suitable solution for their needs. Here are the reasons why we should choose honeypots

- Honeypots can capture attacks and give information about the attack type and if needed, thanks to the logs, it is possible to see additional information about the attack.
- 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.
- 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.
- 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.

CONCLUSION

Any Organization or firm with either outside resources/areas or cloud administrations ought to deploy cloud-based Honeypots. The IT staff might be required to arrange the Honeypots, yet the genuine outline ought to be driven by the security groups will's identity observing for vindictive movement. Any association managing delicate information in the cloud must prefer Honeypots, and they will likewise require talented system heads to screen the logs and respond to the information. There are some incredible open source apparatuses that have been created to help with the observing and log gathering of Honeypots. It clearly relies on the cloud stage itself. "The perfect Honeypot for Amazon EC2 will contrast from Microsoft's Azure or IBM's cloud". In some ways, the customary Honeypots are not perfect as they tend to reflect the more conventional desktop and server working frameworks. They are, be that as it may, definitely best conveyed where fitting security experts are likewise checking and breaking down at all circumstances. The supplementary utilization of human collaboration gives that additional layer of security and the expert may distinguish a potential or hurtful assault that had never been seen and henceforth observing programming would have no learning." One of the best bits of best practice counsel is to redo from the get go. Honeypot innovation is open source thus the awful folks will be exceptionally acquainted with default settings and will screen for these early signs of a trap. These systems must be setup in an environment which care about their customers and want an extra edge in security in their cloud based platform.

BIBLIOGRAPHY

[1] Panagiotis Radoglou Grammatikis, Thomas Lagkas, “Strategic Honeypot Deployment in Ultra-Dense Beyond 5G Networks: A Reinforcement Learning Approach”,IEEE,2022

[2] Radoglou-Grammatikis, A. Liatifis, E. Grigoriou, T. Saoulidis, A. Sarigiannidis, T. Lagkas, and P. Sarigiannidis, “Trusty: A solution for threat hunting using data analysis in critical infrastructures,” in 2021 IEEE International Conference on Cyber Security andResilience (CSR). IEEE, 2021.

[3] Poorvika Singh Negi , Aditya Garg and Roshan Lal “Intrusion Detection and Prevention using Honeypot Network for Cloud Security”,IEEE,2020.

[4] Diamantoulakis, C. Dalamagkas, P. Radoglou-Grammatikis, P. Sarigiannidis, and G. Karagiannidis, “Game theoretic honeypot deploymentin smart grid,” Sensors, vol. 20, no. 15, p. 4199, 2020.

[5] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, “An iot honeynet based on multiport honeypots for capturing iot attacks,” IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3991–3999, 2019.

[6] C. Dalamagkas, P. Sarigiannidis, D. Ioannidis, E. Iturbe, O. Nikolis, F. Ramos, E. Rios, A. Sarigiannidis, and D. Tzovaras, “A survey on honeypots, honeynets and their applications on smart grid,” in 2019 IEEE Conference on Network Softwarization (NetSoft). IEEE, 2019, pp. 93–100.

[7] ChitraRajagopalan. P,TanupriyaChoudhury,Praveen Kumar, A Proposal and Implementation of Algorithm to enhance the security of the cloud”, 5th Fifth International Conference on System Modeling & Advancement in Research Trends,IEEE,2016

[8] Bhaskar Mandal ,Tanupriya Choudhury, “A Secure Biometric Image Encryption Scheme using Chaos and Wavelet Transformations”, International Journal of Advanced Security in Data Analytics and Networks (Special Issue for Recent Advances in Communications and Networking Technology),2016.

[9] Navneet Kambow, Lavleen Kaur Passi, “Honeypots: The Need of Network Security”, International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014

[10] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, “Cloud security issues” In ServicesComputing, 2009. IEEE International Conference on, page 517520, 2009.

[11] Jyatiti Mokube, Michele Adams, “Honeypots: Concepts, Approaches, and Challenges”, Department of Computer Science, Armstrong Atlantic State University,2008.

[12] L. Spitzner, “Honeypots: Tracking Hackers,” Boston, USA: Addison Wesley, Parson Education, ISBN 0 321108957, 2003.