International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

HONEYPOT DEVELOPMENT USING DESIGN THINKING FRAMEWORK

Dr.V.Savitha[1] *,Ramana Vinayak.R*[2]*, Niranjan.R*[2]*, Nandita.R*[2]*, Surya Prasanth.S*[2]

[1]AP/CSE, SNS College Of Technology, Saravanapatti, Coimbatore – 641035, India
[2]SNS College Of Technology, Saravanapatti, Coimbatore – 641035, India

ABSTRACT

Cybersecurity is an evolving challenge, and organizations face continuous threats from sophisticated cyber adversaries. To bolster the resilience of their networks, organizations we deploy a Intrusion Detection Systems (IDS) to detect and respond to potential security incidents using the honeypot development. The honeypot is set of a program which can be set to a cloud, web application & to a application.This research delves into the development and deployment of honeypots specifically tailored for cloud platforms, aiming to enhance threat detection and response mechanisms within cloud infrastructures. Honeypots, intentionally designed decoy systems, play a crucial role in mimicking and analyzing potential cyber threats, thereby bolstering the overall security posture of cloud environments. Even though when some unauthorized activities are detected within the honeypot, security personnel are alerted. This provides an early warning system, allowing organizations to respond quickly to potential security incidents.

Keywords: IDE – Intrusion Detection System

1. INTRODUCTION

Cybersecurity plays a pivotal role in the effective deployment and management of honeypots. While honeypots serve as valuable tools for detecting and studying cyber threats, their implementation requires careful consideration of security principles to prevent unintended consequences. A “Honeypot” is a metaphor that references using honey as bait for a lure or trap. Honeypots have served many purposes in history, including recruiting spies and catching criminals in real life. Honeypots have also long made their way into computing as a way to gather information about potential threats targeting public facing assets. Honeypots are a powerful tool for threat intelligence researchers, security engineers, and malware analysts. Honeypots come in many forms, collecting different information and serving distinct purposes.Honeypots serve a powerful purpose for threat intelligence. Having the ability to collect information from attackers in a controlled environment is an important intelligence asset which can help you always stay one step ahead of stopping real attacks before they happen.Honeypots come in different tiers of interactivity.

2. LITERATURE REVIEW

Paul. A.J, et al. 2007 presented security in a cloud computing environment mostly uses this infrastructure as a service for the research work.They provide opportunities for offering capital cost and focused on core competencies. The purpose of this paper is to use Honey pot as a security tool in a cloud environment. Joshi Ashay Mukundrao et al. 2011 discussed cloud computing is the newly emerging field because of its performance, high availability, least cost. In cloud computing, the data get stored in service providers. This paper has been written to focus on the problem of data security. Stephen Brown et al. 2012 conducted a study using honeypots within various cloud computing platforms such as Amazon EC2, Windows Azure etc. to learn more about what kind of packets they receive. They used multiple honeypots such as Dionaea, Kippo, and Amun on the cloud instances. They gathered data about where attacks came from, what kinds of attacks made, and various cloud instances. Nithin Chandra et.al, 2012 presented a Cloud Security using Honey pots. The concepts were first introduced by several icons in computer security, specifically Cliff Stoll in the book “The Cuckoo's Egg”, and Bill Cheswick's paper “An Evening with Berferd." This paper explained that honeypots are used for securing cloud systems, their advantages and disadvantages etc. Michael Beham et.al, 2013 explained that in many organizations reasonably attractive towards the services which are used in a cloud environment. This study of the security in the cloud environment is assessed by deploying and running Dionaea honeypots for a few months in the cloud provide networks. Hwan-Seok Yang, 2013 explained that in cloud computing, intrusion detection and prevention systems are one such measure to lessen the attacks. Different researchers have proposed different IDSs time to time. Some of these IDS’s combine features of two or more IDSs which are called as hybrid intrusion detection Systems. For a signature based IDS if an attacker attacks slowly and organized, the attack may go undetected through the IDS. Thus, signature-based IDS fail to detect unknown attacks. Hybrid Intrusion Detection System (HIDS) combines the positive features of two different detection methodologies-Honeypot methodology and anomaly based intrusion detection methodology. Navneet Kambow et.al, 2014 said that network forensics is used to notice attacker’s activity and analyze their behavior. This assessment paper is based upon the preface to honeypots, their significance in network security, types of honeypots, their advantages, disadvantages and legal issues connected to honeypots. Huseyin Ulusoy,et.al 2015 gave many research projects from the past, and built intrusion detection systems and honeypot architectures based on virtual machine introspection (VMI). These systems directly provide benefit from the use of virtualization technology. They compare the performance of existing nested virtualization solutions and analyze the impact of the performance overhead on VMI-based intrusion detection and honey pot systems. Ramya. R, cloud 2015 explained in cloud computing, accessing the data from data centers reduces the chances of eavesdropping and storage cost. A honey pot is a system that intentionallydesigns to invite malicious users to enter in the network. Honeypots is used in various cloudcomputing platforms (such as Amazon EC2,Windows Azure etc.) with the objective of learningmore about what kind of packets they receive.

3. PROJECT ANALYSIS

A honeypot is a security mechanism designed to detect, deflect, or counteract attempts at unauthorized use of information systems. It consists of a system or network that appears to be part of a legitimate infrastructure but is actually isolated and monitored, with the purpose of attracting and identifying malicious activity. Honeypots are intentionally deceptive, designed to lure attackers into interacting with them. They may mimic various types of systems, services, or vulnerabilities to appear attractive to potential attackers. Honeypots are typically isolated from the production environment to prevent any impact on critical systems. They operate in a controlled and monitored environment, allowing security professionals to study and analyze the tactics, techniques, and procedures used by attackers. Honeypots are closely monitored to capture detailed information about any malicious activities. This includes logging network traffic, system interactions, and any attempts at exploitation. When unauthorized activities are detected within the honeypot, security personnel are alerted. This provides an early warning system, allowing organizations to respond quickly to potential security incidents. Honeypots are valuable tools in cybersecurity for improving threat intelligence, understanding attack techniques, and enhancing overall security posture to the cloud and the system.

PROBLEM STATEMENT

In the rapidly evolving landscape of cybersecurity, organizations face persistent challenges in proactively identifying and mitigating cyber threats. While traditional security measures provide a baseline defense, there exists a critical need for advanced detection mechanisms that go beyond reactive strategies. The deployment of honeypots, which are intentionally vulnerable systems designed to attract and analyze malicious activity, presents a promising avenue for bolstering threat intelligence in the cloud or web services. Which act like a honey bait for the attackers and also honeypots offer a promising solution for threat detection and intelligence gathering, their deployment in cloud environments presents unique obstacles.

PROPOSED SYSTEM

We have developed our project using the network as the base for the honeypot.The network is the perfect place to host your honeypot because it’s cheap, quick, and flexible. Many cloud providers offer a free tier that includes a free virtual machine or an allowance to spend on cloud resources. A virtual machine is a virtual computer that is able to be developed on a physical server through code. Virtual computers can easily host a service which can be used for the honeypot. we will create a virtual machine via the AWS console. Start by searching for the EC2 service in network.The honeypot system will be designed with a modular and scalable architecture. It will consist of both high-interaction and low-interaction honeypots strategically placed across the organization's network and cloud environments. The architecture will be adaptable to changes in the IT landscape and evolving threat scenarios. Integrate cloud-native honeypots specifically designed for the organization's cloud environments. These honeypots will mimic cloud services, instances, and configurations to attract and analyze cloud-specific threats. Dynamic configuration features will enable seamless adaptation to changes in the cloud infrastructure. This integration will contribute to a more comprehensive defense strategy. The proposed system aims to strengthen the organization's cybersecurity posture by deploying an advanced honeypot infrastructure.

4. PROJECT DESCRIPTION

EXISTING SYSTEM

The existing system includes different types of honeypots, such as high-interaction or low-interaction honeypots. High-interaction honeypots involve real systems that attackers can interact with, while low-interaction honeypots simulate services and capture interactions in a more controlled manner. Examine the effectiveness of the monitoring and logging mechanisms in place. Verify if the system is continuously monitoring interactions, collecting network traffic, and logging system events. Real-time monitoring is crucial for promptly detecting and responding to malicious activity.

WORKING OF PROPOSED METHODOLOGY

We have developed our project using the network as the base for the honeypot. A virtual machine is a virtual computer that is able to be developed on a physical server through code. Virtual computers can easily host a service which can be used for the honeypot. we will create a virtual machine via the AWS console. Start by searching for the EC2 service in network.The honeypot system will be designed with a modular and scalable architecture. It will consist of both high-interaction and low-interaction honeypots strategically placed across the organization's network and cloud environments. Integrate cloud-native honeypots specifically designed for the organization's cloud environments. These honeypots will mimic cloud services, instances, and configurations to attract and analyze cloud-specific threats. Dynamic configuration features will enable seamless adaptation to changes in the cloud infrastructure. To Ensure seamless integration with native security features provided by cloud service providers. Leverage identity and access management (IAM), security groups, and logging services to enhance the honeypot's security capabilities.

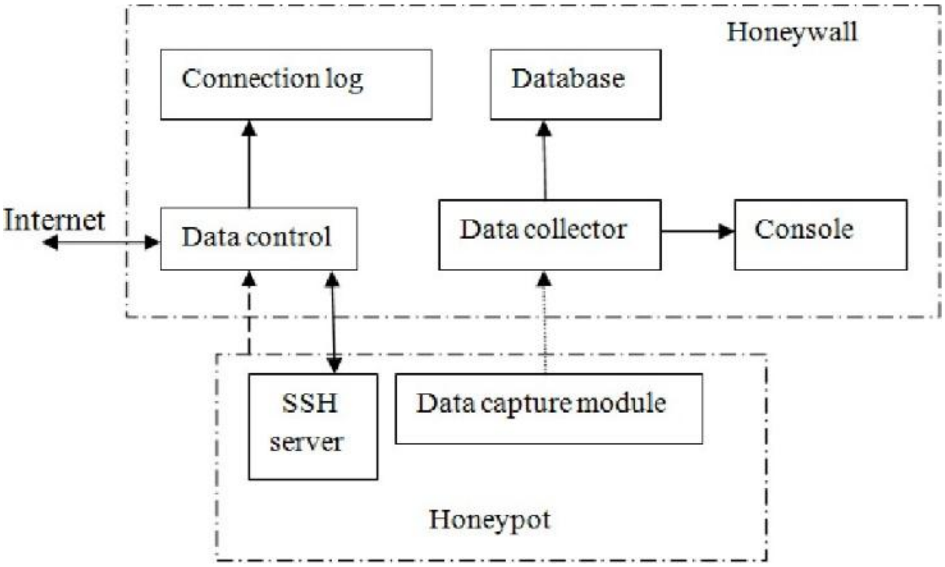

Fig 4.3: Architecture Diagram

5. IMPLEMENTATION

Implementing a honeypot involves creating a sophisticated decoy system or network resource that mimics a legitimate target to attract, detect, and analyze unauthorized access attempts. The primary goal of a honeypot is to gather intelligence on potential attackers, understand their methods, and enhance overall cybersecurity defenses.Begin by designing the honeypot to replicate an actual system or network component. This could be a web server, database, or any other resource that attackers might find attractive. Ensure the honeypot is isolated from your critical infrastructure to prevent any potential damage if the honeypot is compromised. The isolation can be achieved through virtualization, separate physical hardware, or cloud-based environments.Populate the honeypot with services, applications, and data that appear valuable and vulnerable. This might include outdated software, open ports, and deliberately weak security configurations that entice attackers. The goal is to simulate an environment that feels authentic enough to engage attackers for extended periods.Implement robust monitoring tools within the honeypot to capture all interactions, including attempts to exploit vulnerabilities, lateral movement, and data exfiltration. Logging should be detailed, capturing IP addresses, commands executed, files accessed, and any malware deployed. This data is invaluable for understanding the attackers’ techniques, tactics, and procedures (TTPs).Regularly analyze the data collected from the honeypot to identify trends, new attack vectors, and common techniques used by intruders. This intelligence can inform your broader cybersecurity strategy, allowing you to patch vulnerabilities, update security policies, and improve incident response plans.Keep the honeypot updated to reflect current vulnerabilities and emerging threats. This ensures the honeypot remains a relevant and enticing target, providing ongoing insights into the evolving landscape of cyber threats.

6. ADVANTAGES

1. Real-Time Threat Detection

Honeypots provide real-time insights into current attack techniques and malware behaviours. By setting up decoy systems, organizations can capture and analyse ongoing attacks, helping them identify vulnerabilities in their own networks and allowing timely responses.

2. Reduced False Positives

Traditional Intrusion Detection Systems (IDS) often generate high volumes of false positives. Honeypots, on the other hand, capture only unauthorized or malicious activities. Since legitimate users have no reason to access honeypots, any interaction is almost certainly malicious, reducing the chances of false alarms.

3. Forensic Analysis

Honeypots capture detailed logs of attacker activities, which can provide crucial forensic data.

4. Enhances Threat Intelligence

Honeypots contribute to the broader cybersecurity community by sharing attack data and trends. By analysing malware samples and attacker techniques, organizations can contribute to databases that enhance threat intelligence and improve global cybersecurity.

5. Low Resource Consumption

Honeypots typically require minimal resources compared to traditional security tools such as firewalls or intrusion prevention systems.

7. CONCLUSION

The deployment of honeypots within a network emerges as a strategic and indispensable practice. As a deceptive mechanism designed to lure and identify malicious actors, honeypots play a pivotal role in fortifying an organization's defenses, enhancing threat intelligence, and fostering a proactive security posture.Honeypots seamlessly integrate with broader threat mitigation strategies, serving as a proactive defense mechanism. The presence of honeypots not only identifies vulnerabilities but also validates the effectiveness of existing security controls. Organizations can assess the robustness of their defenses, identify potential weaknesses, and iteratively improve their security measures based on tangible insights gained from honeypot deployments.honeypots stand as a linchpin in network security strategies, offering a multifaceted approach to bolstering defenses. Their ability to detect threats early, unravel adversary tactics, contribute to threat intelligence, and facilitate continuous learning positions honeypots as a cornerstone in the modern cybersecurity arsenal. As organizations navigate the complexities of cyberspace, the strategic incorporation of honeypots within network security architectures emerges as not merely an option but a necessity in the pursuit of cyber resilience.

8. REFERENCE

[1] Spitzner, L. 2002. Honeypots: Tracking Hackers. 1"" ed. Boston, MA, USA: Addison Wesley.

[2] Mokube, I. & Adams M., 2007. Honeypots: Concepts, Approaches, anChallenges.ACMSE 2007, March 23-24,2007, Winston-Salem, North Carolina, USA, pp.321-325.

[3] Aaron Lanoy and Gordon W. Romney, Senior Member, IEEE[2006] A Virtual Honey Net as a Teaching Resource

[4] F. A. Shuja. (2005, November). Virtual Honeynet: Deploying Honeywall using VMware, Pakistan Honeynet Project..

[5] Honeywall CDROM Roo 3'd Generation Technology, Honeynet Project & Research Alliance.

[6] G. Romney, ct al., "A Teaching Prototype for Educating IT Security Engineers in Emerging Environments,' Presented at the IEEE ITHET 2004 Conference in Istanbul, Turkey, June 2, 2004. Published in IEEE Xplore.

[7] Cliaord Stoll. Stalking the Wily Hacker. Communications of the ACM.

[8] Ram Kumar Singh & Prof. T. Ramanujam. Intrusion Detection System Using Advanced Honeypots, 2009

[9] Martin Roesch, Snort- Lightweight Intrusion Detection for Networks, Proceedings of LISA*99: 13th Systen Administration Conference, Seattle, Washington USA, 2005

[10] The Honeynet Project. Know Your Enemy: Honeynets (May2005)

[11] Honeynet Research Alliance. Project Honeynet Website.Retrieved May 16th 2003 from the World Wide Web.

[12] Brian Scottberg et-al. Internet Honeypot: Protection or Entrapment, 2002.

[13] The Honeynct Project, Know Your Enemy: Honeynets, April 2001.

[14] The Honeypot Project, Know Your Enemy: Revealing the Security tools, tactic, and motives of Black hats community.2002.

[15] Hybrid Honeypot System for Network Security by Kyi Lin Kyaw, 2008.