ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025
https://doi.org/10.5281/zenodo.15229326

DEPLOYING HONEYPOTS FOR PROACTIVE THREAT MONITORING SOC'S

K.Jothsna[1], Mamidi Nithin Goud[2], Mada Balaji[3], Chinthakindi Bhanu[4], Vasa Varshith Kumar[5]
[1] Associate Professor, Dept. of CS, Sri Indu College of Engineering and Technology, Hyderabad,
[2 3 4] Research Student, Dept. of CS Sri Indu College of Engineering and Technology, Hyderabad

Abstract

In an era of escalating cyber threats, the need for robust defenses against malicious activities is paramount. In this project, we propose a novel approach to leverage honeypots in conju nction with Canary Tokens to accurately pinpoint the geographical locations of attackers. By strategically deploying these decoy resources across diverse network environments, we capture valuable data on unauthorized access attempts and malicious behavior. Through the analysis of Canary Tokens, which act as unique identifiers triggered upon interaction, we can trace the origin of these attacks to specific IP addresses. Utilizing this information, security professionals gain insights into the geographical distribution of attackers, aiding in threat intelligence, incident response, and the implementation of targeted security measures. This integration of project honeypots and Canary Tokens enhances network defense strategies, providing organizations with a proactive stance against cyber threats.

Keywords: Occupational structure, Agriculture sector, Non-agriculture sector, Workers, Non workers, Kerala

I. INTRODUCTION

In today's interconnected world, cyber attacks are on the rise, raising concerns about digital security. To combat this threat, honeypots are deployed as proactive defense measures. A honeypot, a cybersecurity tool designed to mimic vulnerable systems or services, serves as a decoy to attract mitigate potential threats before they can cause significant harm.

However, merely identifying attackers' IP addresses may not provide sufficient insights into their origin or geographical location. To address this limitation, the integration of Canary Tokens with honeypots offers a promising solution. Canary Tokens are unique identifiers strategically placed within a network environment, designed to trigger upon interaction with unauthorized users. By incorporating Canary Tokens into honeypot deployments, we can not only

attackers. By tracking the IP addresses of these attackers, honeypots play a pivotal role in identifying potential threats and discerning patterns of malicious activity. This information is invaluable in fortifying the protection of networks and systems. Honeypots offer a crucial first line of defense, providing organizations with the ability to detect, analyze, and

detect unauthorized access attempts but also ascertain the precise IP addresses of attackers. This data can then be utilized to determine the geographical locations of these malicious actors, enabling security professionals to gain deeper insights into the global distribution of cyber threats. Through the synergistic utilization of honeypots and Canary Tokens, organizations can enhance their threat intelligence capabilities and bolster their defenses against evolving cyber threats.

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

II. LITERATURE SURVEY

In the paper called "Tracking and Tracing Proxy Enabled Systems" a system is developed that determines whether a given IP address is proxy or not and takes into account the country and region as well as IPv4 and IPv6. The initial approach of this system is based on tracing and tracking features in which it will identify the user behind the proxy server. This system is divided into two features which are 1. Tracing feature: In this feature, they used ZMB technique which will help to know about the user i.e., from where the proxy server is used. i.e. its location. 2. Tracking feature: In this feature, they have taken datasets from a community name IP2 and used the SMCH (satellite networks routing handover) algorithm, which is capable of guaranteeing the QoS of the handover and minimizing the operational cost. The SMCH consists of two phases: route augmentation and rerouting. This will work for both IPv4 and IPv6. It will help to know about the last seen of the server and also its proxy type. Some limitations are The proxy's region, not the host's actual IP address was detected, relying solely on IP-based tracking may not provide a complete picture as users can employ various methods to mask their identity.

In the paper " Detection of Anonymising Proxies Using Machine Learning" they used two-class neural network to create a predictive model that can determine whether a given IP address is a proxy or not. The algorithm that was selected for classification of proxy network traffic was the Azure module "Two-Class Neural Network". The trainer mode is the parameter that sets the algorithm. It contains two options, "Single Parameter" and "Parameter Range". The Single

Parameter option allows the user to enter a single value for each of the parameters whereas the Parameter Range option allows for multiple value ranges to be used. The latter was the selected option for the proxy classification problem as the optimal parameter values were unknown beforehand. This is then combined with the module "Tune model hyperparameters" module which performs a parameter sweep over the specified settings and learns an optimal set of hyperparameters. This process is referred to as "tuning". The specification of the hidden layer can either be a fully connected instance, as selected, or it can be defined using a custom script written in the Net# language. The default, fully connected case uses a pre-defined specification for the hidden layer. This results in a neural network which has one hidden layer, an output layer that is fully connected to the hidden layer which is in turn fully connected to the input layer. Some limitations are Resource Intensive and May generate False Positives/

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

False Negative.

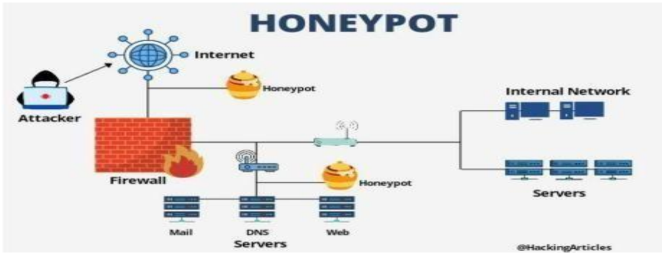
The paper " Detecting Malicious Users Behind Circuit-Based Anonymity Networks " deals with the problem of finding intruders who hide behind anonymity networks that preserve users privacy using SOCKS proxy and Tor. They implemented a per-connection based intrusion detection system (IDS) to detect intruders hiding behind the Tor network and SOCKS proxy chains and validates the detection method with collected SSH and HTTPS connections on the Internet.

The detection performance of this method is excellent with true positive rates in the high 90 percentages and a false-positive rate of less than 2%. This detection method works by monitoring the protocol's handshake process, thus can detect intruders before transmitting the first data packet. Some limitations are Overhead and Latency, False Sense of Security.

The paper " Voyager: Tracking with a Click " a system is developed in order to lure the hacker into clicking on an image or thumbnail that would reveal the hacker's IP address. Voyager a software written in JavaScript is used which handles the creation and logging of a "click bait." when actor requests a page on the Voyager EC2 instance (an AWS virtual server) the application fulfills this request by returning the requested artifact to the actor. Simultaneously, the tcpdump utility logs the actor's request and saves it to a pcap file. Every two minutes the cron job scheduler running on the instance launches the parser.py script. This script proceeds to ingest any pcap files that the tcpdump utility has created since the parser last ran. The parser.py scripts analyzes all the traffic in each pcap file and when the script find a relevant request it logs the associated information to the Voyager database. From the database the request information is viewable by investigators via the event log web view.

Some limitations are Using deceptive methods raises ethical questions and could be considered an invasion of privacy, Clickbait can affect innocent users who may accidentally click on the deceptive content.

III. PROBLEM ILLUSTRATION



IV. PROPOSED METHOD

The proposed system provides contains features of finding IP address and Location of the Attacker. This system can also find the personal details of the attacker and port number and network details in which attacker is working on. This system also ensures the safety of the websites and data.

Provides fast access to find the attackers details in the network. We can also find the details of the documents in which attacker has attacked. Longitude and Latitude of the attackers can be known, which helps us to find the exact details of the Attackers. If attacker downloads any kind of data it gives us as notification.

Step-by-step process for proposed method:

1. Set Up Kali Linux: Install and configure Kali Linux on a suitable system.
2. Design and Deploy Honeypot Website: Develop a website with enticing content to attract potential attackers. Integrate Canary Tokens within the website to act as traps.

3. Implement User Authentication: Implement a login system for the website to restrict access to authorized users only. Provide login credentials to intended users.

4. Monitor Website Activity: Continuously monitor website traffic and interactions to detect any suspicious activities.
5. Capture Attacker Details: When an attacker accesses the website and triggers the Canary Tokens by downloading them, capture their IP address, location, and all other details.
6. Send Notifications to Admin through email: Configure the system to send notifications to the admin whenever an attacker triggers the Canary Tokens.
7. Analyze Attack Patterns: Analyze the gathered data to understand attack patterns, methods, and vulnerabilities exploited by attackers.
8. Enhance Security Measures: Based on the analysis, implement additional security measures to strengthen the system and protect websites and data from future attacks.
9. Continuous Monitoring and Updates: Continuously monitor and update the system to adapt to new attack techniques and ensure ongoing security.

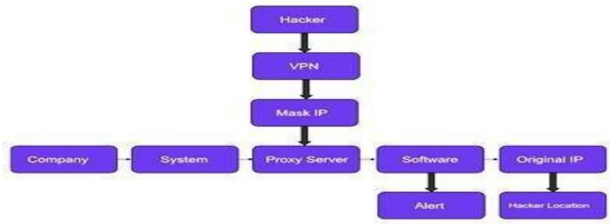
4.1 Modules:

User Module: Every user is provided with their login credentials. They can login and view different documents, data with their login credentials.

4.2 User Interface:

Login page: This the login page of Firm. It has the login option for the users of the commodity. With their login details they can login into their system and view data.
Documents Page: This page contains all the files/documents of the users, it displays all the files associated with the user. It shows in the form of list.

4.3 Proposed Method Illustration



V. CONCLUSION

So, finally I conclude by describing that, this project honeypot represents a significant advancement in cybersecurity measures, offering a proactive defense strategy against potential threats. By utilizing the powerful tools provided by Kali Linux and Canary Tokens, the system demonstrates a sophisticated approach to identifying and neutralizing attackers. Through the deployment of enticing traps within a website, the project effectively lures in potential threats, providing administrators with invaluable insights into their tactics and methodologies.

By capturing crucial details such as the attacker's IP address, location, personal information, and network details, the system empowers administrators to swiftly respond to and mitigate security breaches. The integration of user authentication ensures that only authorized individuals have access to sensitive information, enhancing overall system security.
Moreover, the project's ability to send real-time notifications to administrators upon detection of suspicious activity enables rapid response and mitigation efforts, thereby minimizing potential damage to websites and data. The continuous monitoring and analysis of attack patterns further strengthen the system's effectiveness, allowing for the implementation of targeted security measures to thwart future attacks.

In conclusion, the honeypot project offers a comprehensive and proactive approach to cybersecurity, leveraging advanced techniques to detect, analyze, and mitigate potential threats. By enhancing network security measures and facilitating prompt response to malicious activities, the project contributes to creating a safer online environment for users and organizations alike.

VI. FUTURE SCOPE

This honeypot project lays a solid foundation for future advancements and expansions in several areas that includes:

1. Enhanced Detection Techniques: Incorporating machine learning algorithms or AI-driven analysis can improve the system's ability to detect and differentiate between benign and malicious activities, leading to more accurate threat identification.
2. Advanced Notification Systems: Developing more sophisticated notification mechanisms, such as real-time alerts through mobile applications or integration with Security Information and Event Management (SIEM) systems, can streamline response times and enhance overall situational awareness.
3. Expanded Data Analysis: Integrating big data analytics techniques can enable deeper insights into attack trends, enabling administrators to anticipate and proactively mitigate emerging threats before they manifest into security breaches.
4. Integration with Threat Intelligence Platforms: Integrating the honeypot system with external threat intelligence platforms can provide access to a broader range of threat data and enrich the context of detected incidents, enabling more informed decision-making and response strategies.
5. Automated Response Mechanisms: Implementing automated response mechanisms, such as blocking IP addresses or deploying deception technologies to divert attackers, can further fortify defenses and minimize the impact of cyber threats in real-time.

6. Cloud-based Deployment: Transitioning the honeypot infrastructure to a cloud-based environment offers scalability, flexibility, and cost-effectiveness, enabling seamless deployment across distributed networks and ensuring consistent protection across diverse environments.

7. Integration with DevOps Pipelines: Integrating the honeypot system into DevOps pipelines can facilitate continuous security testing and validation throughout the software development lifecycle, enhancing the resilience of applications and infrastructure against evolving threats.

8. Collaborative Threat Intelligence Sharing: Establishing partnerships with industry peers, cybersecurity communities, and government agencies to share threat intelligence can enrich the collective defense posture and contribute to a more proactive and collaborative approach to cybersecurity.

VII. REFERENCES

[1]. Vipasha Chaudhary, Dr. Purushottam Sharma, Dr Vinod Kr Shukla, Vikas Deep. “Tracking and Tracing proxy enabled system” (ICRITO) Amity University, Noida, India. Sep 3-4, 2021.

[2]. Hane Miller, Kevin Curran, Tom Lunney “Detection of Anonymising Proxies Using Machine Learning” S. International Journal of Digital Crime and Forensics Volume 13, Issue 6, 2021.

[3]. Hou-Hsuan, Stephen Huang, Zechun Cao. “Detecting Malicious Users Behind Circuit-Based Anonymity Networks” S IEEE access Dec 1 2020.

[4]. Samuel Decanioa, Michael Soltysa, Kimo Hildreth “Voyager: Tracking with a Click” KES International. 10.1016/j.procs.2020.08.11.

Cite this article as :
Mrs. M. Sandhya Rani, Guda Ankitha, Polasani Harini, G Ravi, "Cyber Honeypot", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 11 Issue 2, pp. 94-98, March-April 2024. Available at doi :