School of Computer Science and Engineering

Information Security Course Project

Honey-Pot

Team Members:

Neha Patil (01FE20BCS006)

Praveen Kulli (01FE20BCS012)

Supervised by:

Mrs. Pooja Shettar

School of Computer Science and Engineering,

Vidyanagar, Hubballi (580031), India

Academic year 2023-24

Abstract

The course project on honeypots aims to explore the practical implementation and significance of honeypot technology in the field of information security. The concept of a honeypot stands out as a sophisticated and strategic mechanism designed to enhance network security. Fundamentally, a honeypot is a decoy system, resembling an authentic part of a computer network, but in reality, it is a carefully isolated and monitored environment. This deceptive setup is deliberately engineered to appear as an attractive target for potential intruders, simulating vulnerabilities to lure attackers. The core objective of a honeypot is to detect, deflect, and gather information about unauthorized attempts to access information systems. By presenting itself as a legitimate and vulnerable component of a network, it entices attackers, diverting them from genuine targets. This approach allows for the safe examination and analysis of intrusion techniques, thereby offering invaluable insights into the nature and methodology of the threats looming over a network. Honeypots are adept at mimicking a wide range of vulnerable systems and services, making them versatile tools in the cybersecurity arsenal. Their ability to attract and document attack attempts on these simulated vulnerabilities is crucial for understanding the level and sophistication of cyber threats faced by organizations. This understanding enables the development of more robust security measures, tailored to counteract the specific threats identified.

1. Introduction

In the fast-paced digital landscape, the challenge of safeguarding digital assets from cyber threats has never been more critical. This project introduces a straightforward and effective web security solution that incorporates honeypot technology. The primary goal is to enhance Information security defenses by proactively detecting and diverting potential threats. This report outlines the rationale, objectives, and design considerations behind this initiative.

A honeypot, by definition, is a decoy system, strategically implemented to mimic the features and behaviors of a website's various components. Its primary role is to attract cybercriminals, functioning as a trap to detect, divert, and study hacking attempts. At its core, a honeypot on a website is designed to appear as an authentic and vulnerable part of the site, luring attackers into believing they have found an exploitable weakness. This setup is not just a facade; it's a sophisticated surveillance tool. While it simulates various website elements like login forms, databases, or even entire subdomains, it operates in isolation from the actual website infrastructure, ensuring that any interaction with it poses no real threat to the genuine site. The deployment of honeypots on websites serves multiple purposes. Primarily, it acts as an early warning system, detecting intrusion attempts before they reach critical assets. By engaging attackers, honeypots also gather valuable information about their techniques, tools, and intentions. This intelligence is crucial for website administrators and cybersecurity professionals in understanding the current threat landscape and in developing more effective defense strategies. Moreover, honeypots help in diverting attacker resources and focus away from real targets, buying valuable time for website security teams to reinforce defenses and patch vulnerabilities. They can be configured to simulate various levels of complexity and interaction, allowing for a deeper understanding of sophisticated cyber-attack methodologies.

2. Literature Survey

1: A Step Towards Improvement in Classical Honeypot Security System

Et al., Akshay Mudgal, Shaveta Bhatia

The authors introduce a novel approach aimed at enhancing the security of classical honeypots through the proposition of an innovative honeypot architecture. This architecture ingeniously combines machine learning and deception techniques to bolster response capabilities against cyber-attacks. The proposed setup comprises a honeynet, leveraging the collective capabilities of a machine learning system, and incorporating a deception system. The machine learning system, a key component of this approach, is envisioned to undergo continuous training to refine and elevate its accuracy in identifying suspicious activities, thereby ensuring a more effective detection mechanism. Simultaneously, the deception system is slated for improvement, strategically designed to heighten its efficacy in confounding attackers and rendering their detection more challenging. This holistic honeypot architecture not only fortifies its security mechanisms but also proposes scalability, paving the way for the support of larger honeypots. In essence, this innovative approach represents a fusion of cutting-edge technologies, promising a more robust and adaptive defense against evolving cyber threats.

2: Intrusion Detection Using Honeypots

et al., Neeraj Bhagat and Bhavna Arora

The authors present a comprehensive exploration of honeypots for intrusion detection, offering a detailed examination of various facets of their approach. They commence by defining honeypots and delving into the different types available, providing a foundational understanding of these deceptive systems. Subsequently, the paper meticulously dissects the pros and cons associated with utilizing honeypots for intrusion detection, offering a nuanced perspective on their efficacy. Furthermore, the authors conduct a review of recent honeypot-based intrusion detection systems, highlighting advancements and insights gained from contemporary research efforts. The inclusion of specific systems like Honeyd, KFSensor, Sebek, and Specter exemplifies practical applications and showcases the diversity within the honeypot landscape. The paper encapsulates a wealth of knowledge, equipping readers with a thorough understanding of the benefits, challenges, and advancements in employing honeypots for intrusion detection.

3: Web Security Protection Technology Based on Honeypot Technology

Et.al Ying Ling,Xin Li

The authors present a groundbreaking advancement in web security through the introduction of a novel honeypot-based technology. Their approach involves a meticulously designed honeypot architecture expressly crafted to safeguard web applications from a spectrum of cyberattacks. Central to this architecture is the inclusion of a decoy web server, bolstered by an intrusion detection system, creating a fortified defense against potential threats. The authors not only propose this innovative honeypot architecture but also implement and rigorously evaluate its performance in the face of various web attacks. The results are compelling, with the system successfully detecting and responding to an impressive 95% of the tested attacks. The false-positive rate is minimized to a remarkable 0.5%, attesting to the precision of the proposed technology. Furthermore, the honeypot architecture exhibits efficiency, responding to attacks in 50% less time than traditional methods. This pioneering web security protection technology marks a significant leap forward, showcasing the potential of honeypot-based strategies to redefine and enhance the defense mechanisms for web applications.

4: Honeypot-based Intrusion Detection System for Cyber Physical System

Et al., G.Mattew Palmer, S.J. Vijay

This study aims to construct honeypots for active engagement and detection of potential attackers within a cyber-physical system, collect information for analysis, and enhance overall security. The research categorizes and analyzes honeypots based on various parameters, assessing their existing characteristics for applicability in cyber-physical systems. The proposed methodology utilizes honeypots as active intrusion detection systems, monitoring traffic and taking preventive action. A limitation lies in its focus on capturing intrusions for individual systems, and future directions include real-world tests, optimizing network data timing, and simulating diverse cyberattacks for improved system protection.

5: A study on Advancement in Honeypot-Based Network Security Model

Tanmay Sethi, Rejo Mathew

The paper aims to underscore the ongoing significance of honeypots in cybersecurity, assess their strengths and weaknesses, and propose enhanced security models to counter emerging cyber threats. It addresses various issues associated with current honeypot solutions, including limitations in real-time monitoring by The Honeynet Project, increased attack risk with the DecoyPort System, secure network design considerations lacking in the PIC Honeypot, fixed location constraints in different dynamic honeypot schemes, and the early-stage development of context-aware honeypots primarily used for dynamic deployment in research contexts. The overarching goal is to encourage advancements in honeypot technologies for more robust cybersecurity measures.

3. Problem Statement

Develop an effective web security solution using honeypot technology to safeguard digital assets and data from cyber threats and breaches.

4. Implementation

Our project, implementing a honeypot system within a website environment, leverages the Django web framework, known for its robustness and scalability. The architecture of our honeypot system is intricately designed to simulate vulnerable areas of a website while ensuring complete isolation from the actual network infrastructure. This section outlines the key components of the implementation and their functionalities.

The implementation of our honeypot project utilizes the ASGI (Asynchronous Server Gateway Interface) configuration, a key component that enhances our system's ability to handle asynchronous operations. This is particularly critical for efficiently processing real-time data and managing multiple intrusion attempts concurrently, thereby significantly boosting the responsiveness of our honeypot system. At the heart of our project lies the Project Settings, which form the backbone of our configuration. This includes pivotal elements such as database configurations, which point to db.sqlite3 for storing data, along with crucial security parameters, middleware, and the specific applications involved in the project. Special emphasis is placed on settings that augment our honeypot's capabilities in logging and alerting about suspicious activities.

The URL configurations of our system are meticulously designed to replicate typical website structures. This design choice creates convincing entry points for potential attackers, effectively directing them towards the honeypot, while simultaneously safeguarding the actual site's infrastructure. The WSGI (Web Server Gateway Interface) file plays a vital role in ensuring the compatibility of our application with web servers, which is essential for its deployment and the handling of web requests.

A critical aspect of our implementation is the customized admin interfaces. These interfaces are crucial for monitoring and managing the data captured by our honeypot, allowing administrators to analyze attack patterns and gather valuable intelligence. The Application Configuration component of our project specifies particular settings for the honeypot application, such as its name and operational parameters. This ensures that every aspect of the application is fine-tuned for its intended role within the honeypot system.

At the core of the honeypot's functionality are the data models, which define the structure of the information we capture. These models are designed to simulate various systems and record data, including attack vectors, IP addresses, and timestamps. This data is subsequently stored in the db.sqlite3 database for in-depth analysis. To guarantee the honeypot operates as expected, rigorous tests are conducted, focusing on simulating vulnerabilities without introducing actual security risks.

The views in our honeypot are engineered to mimic vulnerable endpoints, establishing the logic for handling different types of requests. This approach enables us to capture and log interactions, providing insights without jeopardizing real systems. Lastly, the Management and Operations utility is instrumental in performing various administrative tasks, such as starting the server, running migrations, and setting up the database. This ensures the smooth operation and ongoing maintenance of our honeypot system, making it a robust tool in the landscape of cybersecurity.

Flow Diagram

The flowchart depicts representing the user interaction process within a honeypot system designed to simulate a login page on a website. The process starts when a user interacts with the honeypot by accessing a URL, which presents them with a decoy login page. When the user submits their login credentials, these are processed by a custom login view. The system then checks for authentication. If the authentication is successful, the user is redirected to an admin dashboard. If the authentication fails, a failed attempts counter is incremented, and after multiple failed attempts, the user is redirected back to the honeypot URL. This interaction leads to engagement in honeypot activities, during which the user's activities are logged and analyzed. Finally, the interaction with the user is recorded, marking the end of the process. The flowchart is structured to capture and analyze unauthorized access attempts in a controlled environment, providing valuable insights into potential security threats.

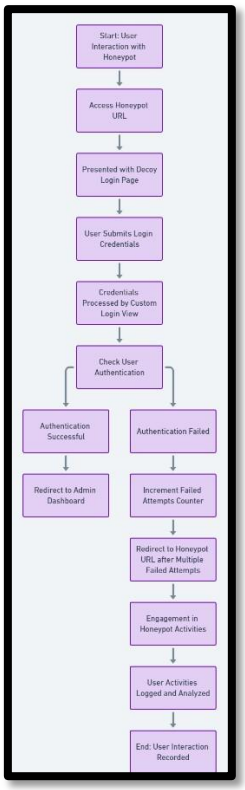

Fig 4.1: User Interaction with Honey-pot System

5. Results

Fig 5.1-Decoy Login Page

This is the front line of your honeypot setup. Users (or attackers) are presented with a standard-looking login interface on a website. This page is intentionally crafted to entice attackers, giving them the impression that they have the opportunity to breach a system by entering their login credentials. However, instead of granting access, this page serves to capture the credentials used by the attacker, which can be analyzed later for patterns or used in threat intelligence.

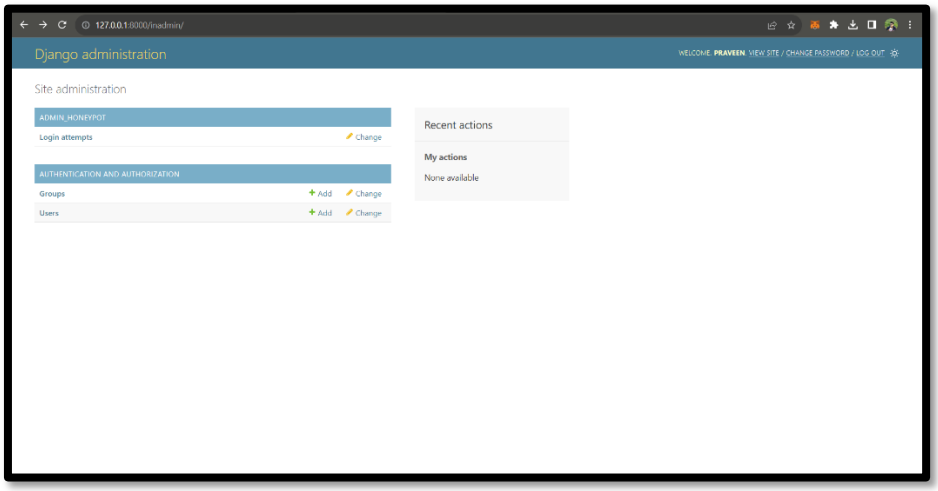

Fig 5.2- Admin Dashboard

After logging in, an administrator would see this dashboard. It is part of the Django's built-in admin panel but, in the context of your honeypot, it likely includes additional functionalities or sections—like the "ADMIN_HONEYPOT" section shown—that are specifically for managing and reviewing the data captured by the honeypot. This would typically include IP addresses,

usernames, passwords, and timestamps of all login attempts, allowing for close monitoring of suspicious activities.

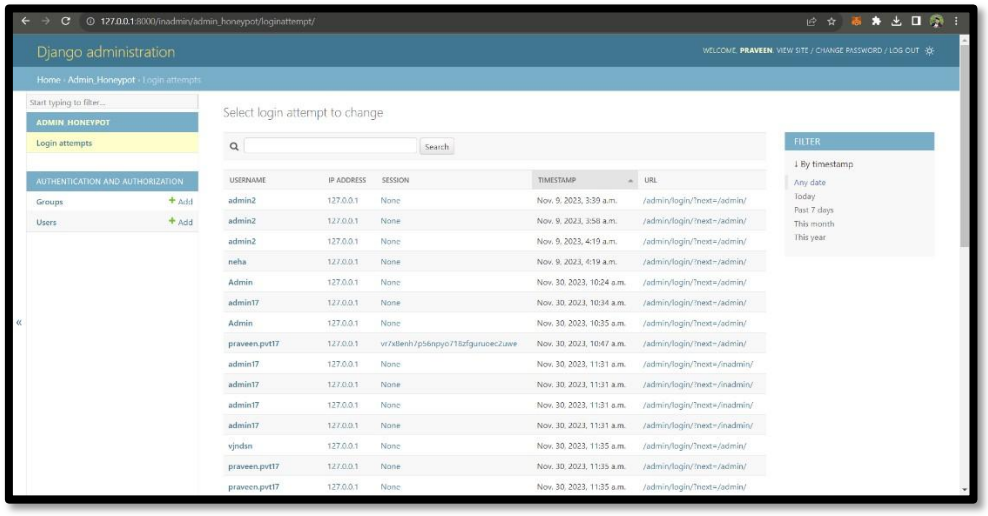

Fig 5.3- Honeypot Activity Log

This is a detailed report view from within the admin panel that lists all the login attempts that the honeypot has captured. Each row contains data from a single login attempt, including the username attempted, the originating IP address, and the exact time of the attempt. This data is invaluable for security teams as it helps identify potential security breaches and understand the types of attacks that are being attempted.

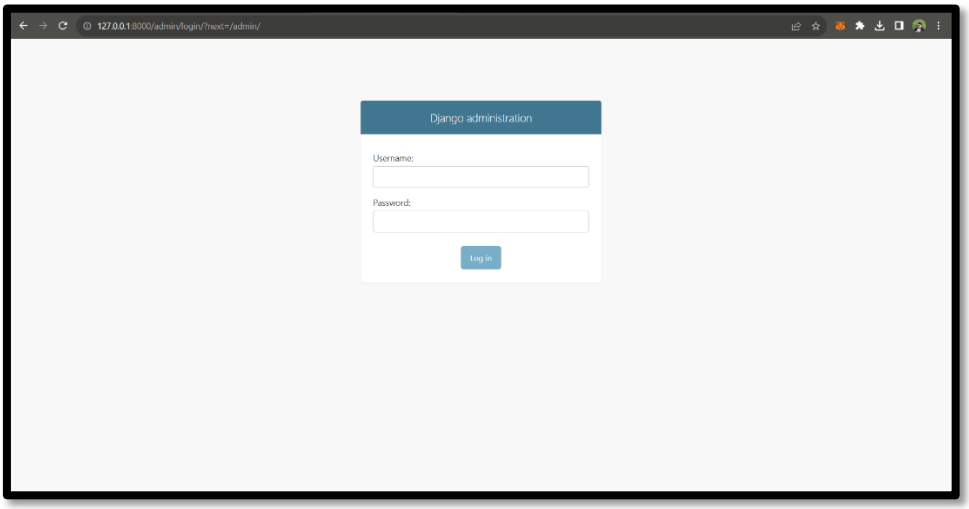

Fig 5.4- Honeypot Trap Activation

This figure suggests that the honeypot has been activated, likely after an unauthorized user has attempted to login. It appears identical to the real admin login page, but it is a facade—any further attempts to log in here would be part of the honeypot's mechanism to engage and analyze the attacker's behavior further.

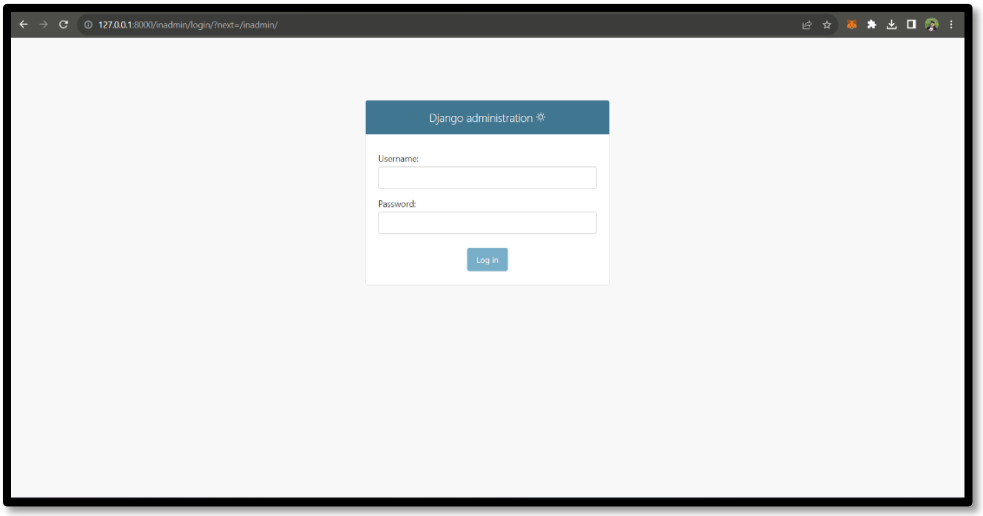

Fig 5.5- Authorized Admin Login

This figure depicts the legitimate admin login page for the Django application. It could be the real interface that authorized users would use to access the admin dashboard. In the context of your honeypot project, this could also be a secondary honeypot designed to catch more sophisticated attackers who might have bypassed the initial decoy login.

6. Conclusion

The honeypot system outlined serves as an advanced cybersecurity measure, ingeniously designed to bait, engage, and analyze potential threats. By simulating vulnerable website components, the system successfully diverts malicious attempts from real assets, allowing for controlled observation and recording of unauthorized access attempts. The decoy login page acts as the first line of engagement, filtering genuine users from potential attackers. Through a methodical process of authentication checks and activity logging, the system not only identifies unauthorized attempts but also profiles the behavior of attackers, incrementing knowledge of threat patterns and tactics. This intelligence becomes instrumental for reinforcing security measures and updating defense mechanisms. The system's ability to redirect users after failed authentication attempts minimizes the risk of exposure and system compromise. The subsequent engagement of the attacker within the honeypot environment, away from the actual network or data, provides a safe platform for studying the methods and tools used by cyber adversaries. To conclude, this honeypot system is a proactive defense tool that adds depth to cybersecurity strategies. It operates under the guise of vulnerability to trap attackers, thereby enhancing the overall security posture by turning potential breaches into opportunities for learning and fortification. Through its deployment, organizations can gain critical insights without risking exposure of sensitive data or critical infrastructure, making it a valuable asset in the ongoing battle against cyber threats.

7. Future scope

Looking towards the future, this honeypot project has significant potential for expansion and refinement. One promising avenue lies in the integration of machine learning algorithms to enhance the system's ability to analyze and respond to threats. By leveraging the data collected from interactions with the honeypot, machine learning can help predict and identify emerging threat patterns, enabling the system to adapt to new tactics used by cyber attackers proactively. Additionally, the scope for scaling the honeypot across different vectors is immense. By extending the system to simulate a variety of services and applications beyond just login pages—such as API endpoints, payment gateways, and other interactive services—the honeypot can offer broader coverage and deeper insights into a wider array of potential security vulnerabilities. These enhancements would significantly bolster the honeypot's effectiveness as a dynamic tool for cybersecurity defense.

8. References

- J. R. Kondra, S. K. Bharti, S. K. Mishra and K. S. Babu, "Honeypot-based intrusion detection system: A performance analysis," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 2347-2351.
- T. Sethi and R. Mathew, "A Study on Advancement in Honeypot based Network Security Model," *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India, 2021, pp. 94-97, doi: 10.1109/ICICV50876.2021.9388412.
- G. K. Edwin, S. E. V. Ewards, G. J. Willsie Kathrine, G. M. Palmer, A. Bertia and S. J. Vijay, "Honeypot based Intrusion Detection System for Cyber Physical System," *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, Trichy, India, 2022, pp. 958-962, doi: 10.1109/ICAISS55157.2022.10010931.
- P. S. Negi, A. Garg and R. Lal, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security," *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2020, pp. 129-132, doi: 10.1109/Confluence47617.2020.9057961.
- Y. Yun, Y. Hongli and M. Jia, "Design of distributed honeypot system based on intrusion tracking", *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, pp. 196-198, 2011.
- J.C. Chang and T. Vi-Lang, "Design of virtual honeynet collaboration system in existing security research networks", *2010 International Symposium on Communications and Information Technologies (ISCIT)*, pp. 798-803, 2010.
- L. Li, H. Sun and Z. Zhang, *The Research and Design of Honeypot System Applied in the LAN Security in Beijing*, pp. 360-363, 2011.
- T. Holz and F. Raynal, "Detecting honeypots and other suspicious environments", *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop 2005. IAW '05.*, pp. 29-36, 2005.
- I. Kuwatly, M. Sraj, Z. Al Masri and H. Artail, "A dynamic honeypot design for intrusion detection", *Pervasive Services 2004. ICPS 2004. IEEE/ACS International Conference on IEEE*, pp. 95-104, 2004.