Intelligent Honeypot Threat Detection and Reputation System Analysis

[1*] M. Arul Sankar, [2]K. Dharmaraj, [3]S. Bharathraja, [4]E. Jeevanath, [5]C. Lingeshwaran

[1,2,3,4,5]Department of Information Technology, Mahendra Engineering College (Autonomous),

Abstract

Honeypots are effective network security systems built to study the tactics of attackers and their intents. In this paper, we deployed honeypot to analyze Secure Shell attacks. Both the dictionary attack and intrusion activities of attackers have been discussed and we collected usernames and passwords that are attempted by dictionary attack targeting Secure Shell service. We have traced the frequently attacking machines based on their IP addresses. We have also recorded the command they executed after successful logins to the Secure Shelf only pot server. We logged a vast amount of connection requests destined to a number of ports originating from different locations of the world. From our honeypot system, we have collected attack data that enables us to. Index Terms—Secure Shell, Dictionary Dionaea, Honeypot, Intrusion. This honeypot involves the design, development, and deployment of a low-interaction, SSH honeypot to attract detect, and analyze automated and manual cyberattacks in real-time. The honeypot acts as a decoy system, mimicking a vulnerable SSH service to lure attackers away from legitimate network resources. The primary goal is to gather threat intelligence, including attacker IP addresses, usernames, passwords, and executed command attempts, without compromising actual production systems. The project will utilize tools like shodan and virus total or a custom script built with a Python library and deploy it on a virtual private server (VPS) for exposure to internet traffic. SSH honeypot infrastructure, leveraging techniques such as emulation and deception to lure potential attackers.

INTRODUCTION

Honeypot is a comprehensive project aimed at developing a robust SSH honeypot system tailored for threat monitoring and detection. This endeavor involves the meticulous design and implementation of an SSH honeypot infrastructure capable of emulating authentic SSH services while effectively luring and monitoring malicious empowers security professionals to create a controlled environment that mimics a real SSH server. This strategic deception lures attackers, allowing for close observation and analysis of their tactics and tools. By meticulously logging all attacker activity within the honeypot, honeypot offers valuable insights into emerging threats and attacker behavior patterns. This enables security teams to identify and neutralize potential threats before they can infiltrate real systems. The intelligence gleaned from Secure Shell empowers organizations to fortify their security posture by pinpointing vulnerabilities and implementing robust security measures to prevent future attacks. As cyber threats constantly evolve, honeypot emerges as a powerful framework for crafting SSH honeypots to monitor threats. By creating a controlled, decoy SSH server environment, Secure Shell allows security professionals to observe and analysis attacker behavior. This comprehensive intelligence empowers teams to proactively identify and neutralize threats before they infiltrate real systems, ultimately fortifying an organization's security posture through informed decision-making and improved threat hunting capabilities. In the face of a relentless barrage of cyberattacks, Secure Shell empowers security professionals with a powerful framework for crafting SSH honeypots – deceptive yet highly realistic SSH server environments designed to lure in threat actors**.** By meticulously logging every move attackers make within this controlled space, honeypot grants security teams deep insights into attacker behavior, including login attempts, executed

commands, and accessed files.

Literatuer Survey

1. **Title:** A Highly Interactive Honeypot-Based Approach to Network Threat Management.

Authors: Xing yuan Yang In this paper, considering the problem that the common defensive means in the current cyber confrontation often fall into disadvantage, honeypot technology is adopted to turn reactive into proactive to deal with the increasingly serious cyberspace security problem. We address the issue of common defensive measures in current cyber confrontations that frequently lead to disadvantages. To tackle the progressively severe cyberspace security problem, we propose the adoption of honeypot technology to shift from a reactive to a proactive approach. This system uses honeypot technology for active defense, tempting attackers into a predetermined sandbox to observe the attacker's behavior and attack methods to better protect equipment and information security performs a variety of advanced functions, such as network threat analysis, virtualization, vulnerability perception, tracing reinforcement, and camouflage detection.

2. **Title**: Analysis and implementation of honeypot Framework for Enhancing Network Security.

Authors: Firoz Mridha, and Md Kamruddin Nur. An overwhelming number of individuals of are using the Internet for a variety of activities such as email, online shopping, bill payments, gaming, and exploration as it becomes more and more ingrained in daily routines around the world. While this technological development has enhanced human existence and increased economic opportunities, it has also sparked the discovery and widespread use of numerous techniques by attackers to get around computer networks

other operations, it is easy to maintain and upgrade the system, while reducing the difficulty of using honeypots. The high interactivity honeypot technology not only attracts attackers into pre-set sandboxes to observe their behaviour and attack methods, but also performs a variety of advanced functions, such as network threat analysis, virtualization, virtualization .

3. **Title**: Honeypot and cyber deception as a tool for detecting cyber-attacks on critical infrastructure

Authors: Morozov , Vakaliuk , Yefimenko , Nikitchuk , Kolomiiets The threat of cyberattacks on critical infrastructure, as well as the growing importance of IoT systems, requires the search for effective mechanisms for detecting and preventing such attacks. This is a worldwide trend and a solution to this problem must be found now. One of the most promising approaches to detecting attacks on both critical infrastructure objects and industrial CFS and IIoT networks is the use of cyber deception systems and complex honeypot solutions. These systems can be

4. **Title:** A Multistage Framework for Honeypot Fingerprinting

Authors: Shreyas Srinivasa And Jens Myrup Pedersen, Aalborg University Emmanouil Vasilomanolakis Honeypots are decoy systems that lure attackers by presenting them with a seemingly vulnerable system. They provide an early detection mechanism as well as a method for learning how adversaries work and think. However, over the past years, several researchers have shown methods for fingerprinting honeypots. This significantly decreases the value of a honeypot; if an attacker is able to recognize the existence of such a system, they can evade it. Thus, a bank model which provides security by using Facial and retina and face verification software by adding up retina and face recognition systems.

5. **Title**: Detection and Analysis of Active Attacks using Honeypot

Authors: Waqas Ahmad, Muhammed Arsalan Raza information system resource called a honeypot is one whose value comes from being used illegally or unauthorizedly. Any interaction with a honeypot is assumed to have malicious intent because attacker thinks it is a vulnerable system and it can be attacked easily. As techniques of network protection, firewalls and Intrusion Detection and Prevention Systems (IDPS) are well known. All of these techniques have some

limitations. But honeypot offers an alternative strategy, it traps the attackers because of its deceiving nature. In firewall would allow only authorized traffic to enter or leave the private network, but it gathers large amount of data that an administrator would find prohibitive to analyse. On the other hand, a honeypot will only collect the data of log attacks to a target host.

METHODOLOGY

A honeypot setup workflow involves identifying a target network, deploying a decoy system that mimics real services, routing attacker traffic to the honeypot, collecting forensic data on attacks, and analyzing the data to improve security defenses. The process begins with defining the goals of the honeypot, such as detecting new attack vectors or studying attacker behavior, and then selecting an appropriate honeypot type and configuration. Traffic is then directed to the honeypot, which logs all interactions for later analysis to understand adversary techniques and develop countermeasures.

1. **Define Objectives**:

   Purpose: Determine why you are deploying the honeypot gather threat intelligence, study attacker methods, distract attackers from real systems, detect new malware. Target: Decide what types of attacks or adversaries you want to attract.

2. **Choose the Honeypot Type**:

   Low-Interaction: These systems emulate common services and are easy to deploy but offer limited data. High-Interaction: These provide more realistic environments, capture detailed forensic data, but are complex to set up and manage. Virtualization: Use tools like to create isolated, vulnerable-looking environments for testing within a real system.

3. **Deploy the Honeypot:**

   Provision Infrastructure: Set up the server, virtual machine, or container for the honeypot. Install & Configure: Install the chosen honeypot software T-Pot for a comprehensive suite and configure its services to mimic real systems, like web servers, databases, or filesharing services.

4. **Isolate and Protect**:

   Network Segregation: Place the honeypot in a carefully controlled network segment, separate from your production environment. Monitoring Tools: Integrate it with an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) for early detection of interactions with the honeypot, and to prevent the honeypot from being used to launch attacks against your production systems.

5. **Attract and Monitor**:

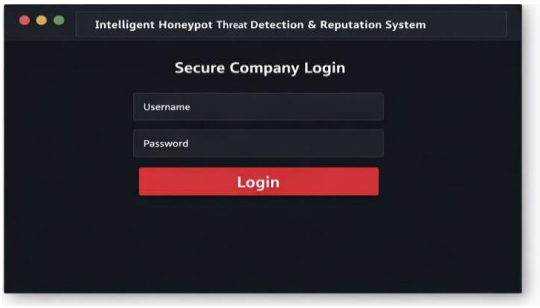
   Traffic Redirection: Route incoming network traffic that seems suspicious or targets specific services towards the honeypot.

RESULT AND DISCUSSTION

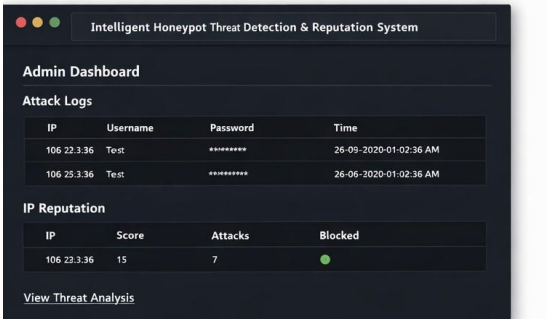
Attack Data & Threat Landscape: Report the types of attacks and reconnaissance attempts observed against the honeypot, including the services or applications targeted. Quantify the frequency and volume of these interactions.

- Attacker TTPs: Detail the Tactics, Techniques, and Procedures (TTPs) used by attackers, such as the specific tools, scripts, or exploits they employed.
- Malware Samples: For a malware analysis honeypot Discuss the role of the honeypot in deceiving adversaries, diverting them from actual production systems, and potentially deterring them from attacking by raising their awareness of active defenses. list the number and types of malware samples collected, along with their characteristics (like MD5 hashes).
- Skill Level & Motivation: Analyze the sophistication and intent of the attackers based on their activities within the honeypot.
- Alerts & False Positives: Report on the number of alerts generated and the percentage of these that were actual threats versus benign activity, demonstrating the effectiveness of the honeypot in reducing false positives

Step1: setting the backend honeypot through (./run.sh)



Step 2: setting frontend honeypot through the honeypot frontend (./run.sh)

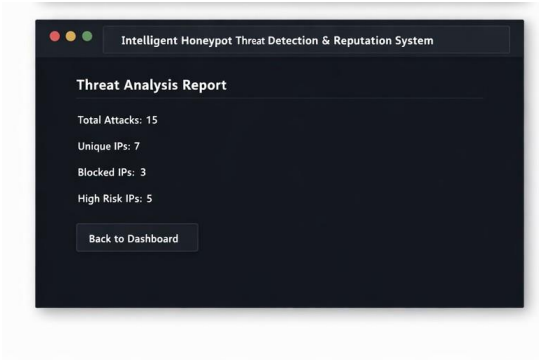


Step 3: ssh root@localhost -p 2222

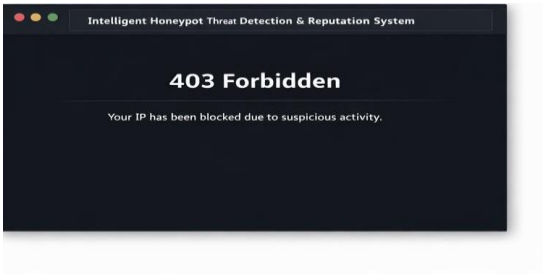
***echo**

***root**

***whoami**



Step 4: It shows live feed attack with a virus total and shodan tools.



FUTURE ENHANCEMENT

*Integration with Machine earning for predictive threat analysis

*Automated blocking of high-risk IPs

*Real-time alert integration (Email/SMS)

*Cloud-based scalable honeypot deployment.

CONCLUSION

- This project successfully designed and implemented an Intelligent Honeypot System for effective threat detection, attacker reputation assessment, and system analysis. The honeypot approach enabled proactive identification of malicious activities by attracting attackers to decoy services, thereby eliminating risks to real production systems.

- The system efficiently captured attacker interactions and analyzed them using threat detection techniques to identify malicious behavior such as brute-force attacks, port scanning, and suspicious payloads. By incorporating a reputation-based evaluation mechanism, the system classified attackers into different risk levels, allowing security administrators to prioritize threats based on severity and frequency.

- Additionally, the system analysis and visualization modules transformed raw attack data into meaningful insights, helping administrators understand attack patterns, targeted services, and temporal trends. Compared to traditional security mechanisms, the proposed solution provides deeper behavioral intelligence and improved situational awareness.

REFRENCES

[1] C. Talos, Talos Year in Review 2022, 2022. URL: https://blog.talosintelligence.com/ talosyearin-review-2022.

[2] N.M.Lobanchykova,I.A.Pilkevych,O.Korchenko,AnalysisandprotectionofloTsystems: Edge computing and decentralized decision-making, Journal of Edge Computing 1 (2022) 55– 67. doi:10.55056/jec.573

[3] D. Fraunholz, M. Zimmermann, H. D. Schotten, Towards Deployment Strategies for Deception Systems Unsupervised Machine Learning, Advances in Science, Technology and

Engineering Systems Journal 2 (2017) 1272–1279. doi:10.25046/aj0203161

[4] D. Fraunholz, H. D. Schotten, Defending Web Servers with Feints, Distraction and Obfuscation, in: 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp.21–25. doi:10.1109/ICCNC.2018.8390365

[5] D. Reti, D. Fraunholz, J. Zemitis, D. Schneider, H. D. Schotten, Deep Down the Rabbit Hole:On References in Networks of Decoy Elements, in: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),2020, pp.1–11. doi:10.1109/CyberSecurity49315.2020.9138850

[6] D. Fraunholz, D. Krohmer, H. D. Schotten, C. Nogueira, Introducing Falcom Multifunctional High-Interaction Honeypot Framework for Industrial and Embedded Applications, in: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2018, pp. 1–8.

[7] D. Fraunholz, D. Krohmer, S. D. Anton, H. Dieter Schotten, Investigation of cyber-crime conducted by abusing weak or default passwords with a medium interaction honeypot

[8] A. Acien, A. Nieto, G. Fernandez, J. Lopez, A Comprehensive Methodology for Deploying IoT Honeypots, in: S. Furnell, H. Mouratidis, G. Pernul (Eds.), Trust, Privacy and Security in Digital Business, volume 11033 of Lecture Notes in Computer Science, Springer International Publishing, Cham, 2018, pp. 229–243. doi:10.1007/978-3-319-98385-1_16.

[9] H. Šemić, S. Mrdovic, IoT honeypot: A multi-component solution for handling manual and Mirai-based attacks, in: 2017 25th Telecommunication Forum (TELFOR), 2017.