Creation of a Honey Pot to Capture and Evaluate Cyber Threat

Department of Computer Science, Stephen F. Austin State University

[1] Ofuafo Orumeteme, Faculty Mentor. [2*]Dr. Pushkar Ogale, [3]Dr. Jianjun Zheng, [4]Dr. Christopher Ivancic

[1]Email: orumetemo@jacks.sfasu.edu , [2*]Email: ogalep@sfasu.edu

Abstract

In the current dynamic threat environment, it is crucial to implement proactive defenses to comprehend attacker behavior. This project introduces a tailored honeypot system that simulates SSH, HTTP, and SQL services to lure and observe cyberattacks. The objective is to identify malicious activities, examine attacker methodologies, and categorize threats utilizing the MITRE ATT&CK framework. Logs were collected and enriched with geolocation data, then analyzed via Splunk. The result is a fully functional honeypot environment capable of profiling attackers, visualizing trends, and evaluating threats. This demonstrates the value of honeypots in identifying vulnerabilities and enhancing detection capabilities in cybersecurity operations.

Introduction

Technological advancement in the last decade has had its own attendant consequences. The risk of cyber attacks to individuals and organization has grown exponentially due to technological advancement. While conventional defenses such as firewalls and antivirus software are reactive, honeypots provide a proactive approach for monitoring attacker behavior in a controlled setting. This project entails the configuring of a multi honey pot system that emulates SSH, HTTP, and SQL services. The goal is to capture real-world cyberattack and analyzed the data using Splunk to gather threat intelligence and to gain deeper knowledge into attacker's behavioral pattern. The MITRE ATTACK Frame work will be used as a guide to mapped out attacker's behavior and a real time Flask dashboard for visualization of attacks. The system, hosted in AWS Cloud, illustrates how honeypots enhance proactive cybersecurity through threat visibility, attacker profiling, and structured analysis in accordance with industry standards.

Objective

- Simulate SSH,HTTP, and SQL services to attract real-world cyberattacks
- Capture and store attacker interactions for structured analysis
- Analyzed captured data using Splunk Cloud
- Map observed behaviors to MITRE ATTACK techniques and tactics
- Visualize attack patterns using a custom-built Flask dashboard
- Demonstrate the role of honeypots in proactive cyber threat evaluation

Honeypot Threat Analysis Workflow:

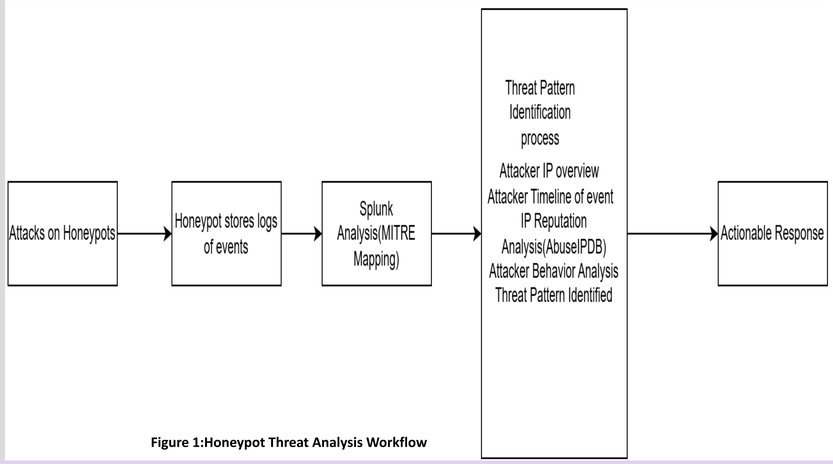

Figure 1:Honeypot Threat Analysis Workflow

Methods and Materials

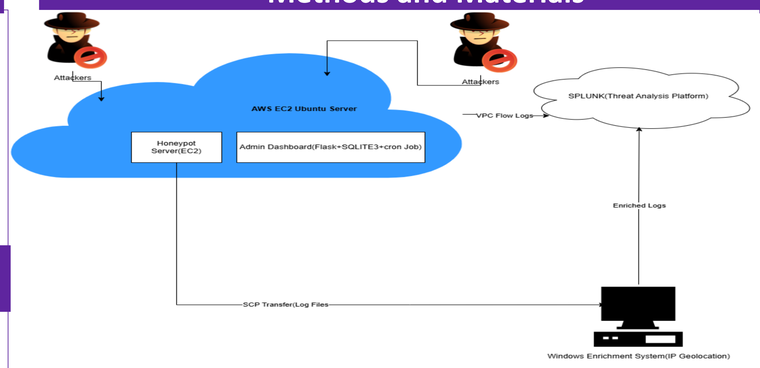

Figure 2: Solution Architecture

Honeypot Setup: Honeypots were deployed to simulate vulnerable **SSH**, **HTTP**, and **SQL** services. These were hosted on an AWS EC2 instance running Ubuntu and configured to attract and log real-world attacker interactions. Security Considerationlet

Log Collection and Analysis: Event logs generated by the honeypots were collected and analyzed using **Splunk Cloud**. This enabled pattern recognition, attacker behavior profiling, and MITRE ATT&CK technique classification across different attack surfaces.

Flask Dashboard: A custom-built Flask web dashboard was developed to **visualize and monitor** honeypot activity in near real time. It displayed attacker IPs, MITRE technique breakdowns, login attempts, geolocation maps, and event trends, providing a live view of evolving threats.

Attack Summary

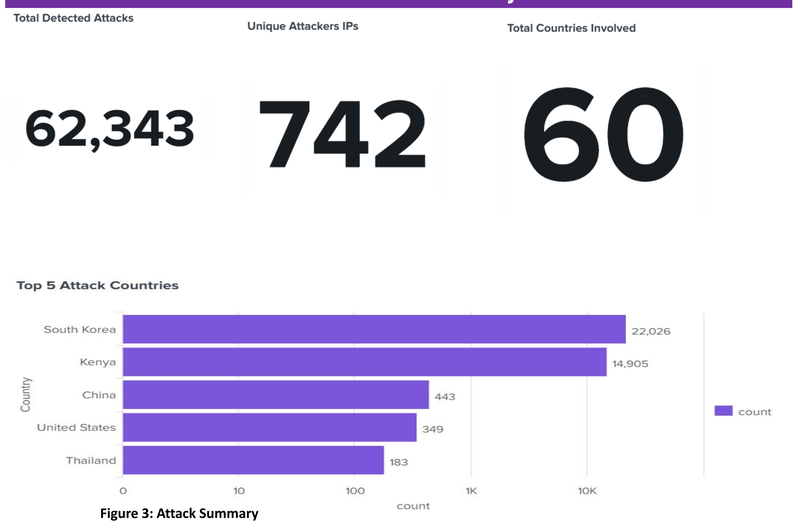

Figure 3: Attack Summary

Results

The honeypot captured real-world SSH, HTTP, and SQL attacks, revealing brute-force, web scanning, and database probing behaviors. Honeypot passwords were analyzed against a 2,000,000-entry subset of the 14,344,391-entry RockYou list, identifying widespread use of common credentials. Events were mapped to 32 MITRE techniques, including T1110.001 and T1595.002. Attackers came from over 60 countries. Top IPs were investigated and blocked. A custom Flask dashboard enabled real-time threat monitoring.

Geographical Distribution of Attack

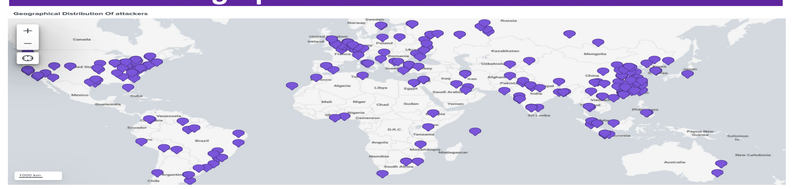

Figure 4: Geographical Distribution of Attacks

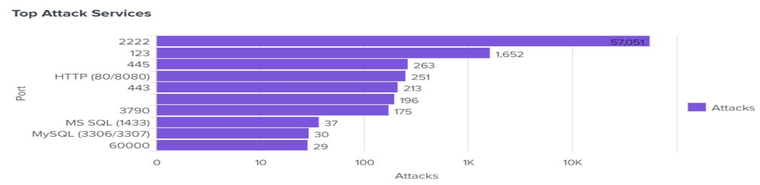

Figure 5: Top Attacked Services

Threat Evaluation: Prevalence of Dictionary Attack Indicators (RockYou Comparison)

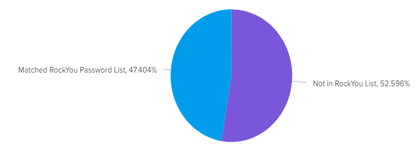

Figure 6: Dictionary Attacks Comparison

Event Log Table — Filter by Date: mm/dd/yyyy

Timestamp	Source IP	Protocol	Port	Event Type	MITRE Technique	Severity	Description
2025-04-30T06:34:10.378825Z	47.222.187.78	ssh	2222	Command Execution	T1059	medium	ls
2025-04-30T06:33:51.514676Z	47.222.187.78	ssh	2222	Command Execution	T1059	medium	uname
2025-04-30T06:30:55.609452Z	47.222.187.78	ssh	2222	Command Execution	T1059	medium	ls
2025-04-30T06:30:32.191192Z	47.222.187.78	ssh	2222	Login Attempt	T1110.001	high	root/123456123456

Figure 7: Flask Dashboard Event Log Table

Conclusions

The project successfully established a honeypot-based environment for the capture and assessment of real-world cyber threats. Various attack vectors were identified targeting SSH, HTTP, and SQL services, encompassing credential assaults, reconnaissance operations, exploitation endeavors, and malware dissemination. The identified threats were categorized and examined utilizing the MITRE ATT&CK framework, yielding significant insights into adversary behaviors and methodologies throughout various phases of the cyber kill chain. The results illustrate the efficacy of honeypots in surveilling, classifying, and comprehending contemporary cyber threats.

Acknowledgement

I extend my deepest gratitude to Dr. Pushkar Ogale, my practicum advisor, for his invaluable guidance and support throughout this project. My appreciation also goes to committee members Dr. Jianjun Zheng and Dr. Christopher Ivancic, whose insights and feedback were instrumental in shaping this research. I am also thankful to my peers and the faculty at the Department of Computer Science, Stephen F. Austin State University, for their encouragement and constructive criticisms.

References

[1] Yang, X., Yuan, J., Yang, H., Kong, Y., Zhang, H., & Zhao, J. (2023). A Highly Interactive Honeypot-Based Approach to Network Threat Management. Future Internet, 15(4), 127. https://doi.org/10.3390/fi15040127

[2] MITRE Corporation. (2023). MITRE ATT&CK® Framework. Retrieved from https://attack.mitre.org/

[3] Morić, Z., Mršić, L., Kunić, Z., & Đambić, G. (2024). Honeypots in cybersecurity: Their analysis, evaluation and importance. Preprints.org. https://doi.org/10.20944/preprints202408.0946.v1

[4] Chandrashekar, K., & Jangampet, V. D. (2024). Honeypots as a proactive defense: A comparative analysis with conventional anomaly detection systems. International Journal of Computer Engineering and Technology (IJCET), 10(5), 213–221. Retrieved from https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_10_ISSUE_5/IJCET_10_05_021.pdf

[5] Spitzner, L. (2003). Honeypots: Tracking Hackers. Boston, MA: Addison-Wesley Professional.

[6] Splunk Inc. (2024). What is Splunk? Retrieved from https://docs.splunk.com/Documentation/Splunk/latest

[7] Amazon Web Services. (2024). Getting started with Amazon EC2 Linux instances. Retrieved from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html