TARGETED HONEYPOT DEPLOYMENT FOR ANALYZING AND MITIGATING THREATS

DR.G.ARAVIND SWAMINATHAN

PROFESSOR AND HEAD/CSE

Computer Science and Engineering

Francis Xavier Engineering College

Tamil Nadu,India

aravindswaminathan.g@francisxavier.ac.in

Ms.M.SOWNDARYAA

Electronics and Communication Engineering

Francis Xavier Engineering College

Tamil Nadu,India

sowndaryaam.ug.21.ec@francisxavier.ac.in

Abstract ---

Cyber threats continue to evolve, posing significant risks to small and mid-sized businesses that often lack the financial resources for advanced cybersecurity. With the rise of sophisticated attack techniques like brute-force attempts, ransomware infections, and credential stuffing, these businesses become prime targets due to weaker security postures. This project deploys a targeted honeypot system using Cowrie,a medium-interaction SSH honeypot, to analyze SSH brute-force attacks and study potential ransomware tactics. By acting as a decoy, the honeypot captures attacker activity, including login attempts, command executions, and malware injection techniques, providing valuable threat intelligence.

Unlike traditional reactive security measures, this proactive approach identifies attack patterns before they can be exploited. The insights gained help businesses refine security strategies, strengthen authentication mechanisms, and anticipate threats without requiring significant financial investment. While real-time ransomware execution monitoring was not implemented due to security risks and time constraints, the honeypot remains a crucial tool in cybersecurity research. The findings from this study emphasize the importance of continuous monitoring, threat intelligence gathering, and proactive security measures in mitigating evolving cyber threats.

I. INTRODUCTION

With ever-evolving cyber threats, small and medium enterprises are still at risk because of their limited technical and financial capabilities.[1]Honey pot-based intrusion detection methods provide an additional layer of security and enhance network performance. These organizations are the preferred target for highly sophisticated attacks, including SSH brute-force attacks, ransomware infections, and credential stuffing.[2] This study aims to examine the performance of the k-Nearest Neighbours (k-NN) and Decision Tree algorithms by contrasting their precision, recall, and F1 score. Traditional security appliances, including firewalls and intrusion detection systems, are typically reactive in their nature, identifying and disabling threats only after they have entered an organization.[3]The lack of synchronization by a worst-case optimization in which the queries made by multiple adversarial agents are received in the worst possible order for the adversary, resulting in a min–max formulation. To overcome this, the installation of a honeypot system intended for deployment through Cowrie has been proposed as a proactive security measure. [4]The proposed method, which works in a black-box way and covers some shortages of the existing adversarial attack methods based on generative adversarial networks .This project entails the use of a medium-interaction SSH honeypot for luring and dissecting brute-force attacks, logging unauthorized logins, command executions, and potential vectors of malware injections.[5]Compared to traditional security equipment, the system provides insightful threat intelligence for helping companies pre-emptively prevent attacks.

As a decoy system, the honeypot invites attackers to engage an emulated vulnerable system, thus enabling the monitoring of their attack patterns by security teams for strengthening real-world defenses.

[6] In the monitoring resource, each level of attack brute force resource used by GHOST is increasing. The execution monitoring of ransomware was possible in real-time, the feature was not utilized given the security and time constraints.[7] The log of intruder activities is maintained which is processed and graphically visualized using ELK. Still, the honeypot remains a crucial device for cyber-security research in search of threat mitigation at lower costs.[8] This paper aims to improve knowledge about the SSH honeypot Cowrie, presenting both knowledge that aids in understanding its architecture and improvements. Aside from being used as a decoy against cyber threats, the honeypot system under attack offers some additional extended advantages that improve security measures for small and mid-sized enterprises. Among the most significant benefits is threat actor profiling.[9] In this study, SSH Telnet honeypot was established using Cowrie software. Attackers attempted to connect, and attackers record their activity after providing access. The system's customizable deployment ensures adaptability across different environments, including cloud-based, on-premises, and hybrid setups, providing flexibility based on business needs.[10] This framework is proposed to detect the ransomware using the "Kaspersky" anti-malware tools and a virtual machine to prevent ransomware attacks. The honeypot's role as a decoy system for attackers misleading threat actors into engaging with a controlled environment.[11]Ransomware establishes unauthorized network connections, both inside the compromised network and externally. This approach reduces the risk of immediate damage while capturing valuable intelligence on attack techniques.**.[**12] Files belonging to the victim are encrypted, rendering them unavailable, and a ransom demand is made to unlock them.

II. LITERATURE SURVEY

As emerging cyber threats arise, small and medium businesses become increasingly vulnerable as they possess limited security controls and limited budgets. Small and medium-sized businesses are the most prevalent targets for SSH brute-force attacks, ransomware infections, and credential stuffing as they cannot implement sophisticated defense tools.

Conventional security devices such as firewalls and intrusion detection systems are usually reactive and act on threats after they have already breached a system. Conventional security devices provide no information regarding attacker techniques, and thus it is not possible to identify and block emerging threats.To counter this threat, the deployment of an interactive honeypot system using Cowrie has been an active security practice.

It is a medium-interaction SSH honeypot, mimics a vulnerable host to entice attackers to engage with a controlled environment. By detecting brute-force attacks, commands being executed, and the possibility of malware injection, the honeypot offers real-time feedback on attack patterns and most exploited vulnerabilities.

Cybersecurity research studies highlight the efficacy of honeypots in threat behavior learning and security policy optimization. Moreover, the deployment of log analysis and monitoring methods optimizes incident response, enabling organizations to enhance authentication mechanisms and deny unauthorized access. In the end, this proactive, affordable security strategy improves overall cyber resilience by assisting firms in identifying and reducing cyberthreats before they become more serious.

III. PROPOSED FRAMEWORK

The Honeypot Threat Analysis and Mitigation System is engineered to operate as a decoy system that emulates vulnerabilities so that attacker activity can be inspected and possible threats can be discovered in real time. The Cowrie honeypot deployment, simulated targeted attacks, and end-to-end threat mitigation processes. As opposed to traditional security systems that depend on passive observation, this system uses a dynamic and interactive deception strategy to deceive attackers and gather useful security information. By interacting with attackers in a simulated environment, organizations can get insight into normal attack vectors, hijacked credentials, and malicious activities and use this information to update their access control policies, authentication systems, and intrusion detection rules. Moreover, it allows customizable attack simulation, allowing security teams to configure SSH banners, credentials, and system responses to simulate real-world enterprise environments and thereby record a broad variety of attack techniques.

One of the integral features of the system is that it deploys Cowrie, a medium-interaction SSH and Telnet honeypot that catches unauthorized access attempts, harvests stolen credentials, and makes notes on attacker interactions. By mimicking an entirely operational SSH setting, Cowrie logs performed commands, payload deliveries, and file exchanges and gives vital knowledge about attack methods. To further enhance its threat analysis functionality, the system incorporates Samba, which emulates a vulnerable file-sharing service to serve as a lure for ransomware attacks. This configuration allows security teams to learn how ransomware spreads, encrypts files, and communicates with shared network resources, helping to improve more effective mitigation techniques

Step 1: Honeypot Deployment Module

- System Initialization: The honeypot system is initialized with Cowrie to mimic weak services (Telnet and SSH).
- Input Validation: Guarantees that the system is designed to process attack traffic without impacting the real production environment.
- Deceptive Services: Cowrie imitates regular services like SSH, FTP, etc., in order to attract the attackers.
- Traffic Monitoring: Traffic is captured and recorded to monitor malicious activity against the honeypot system.

Step 2: Attack Detection Module

- SSH Brute-Force Simulation: The system identifies and records SSH brute-force attacks against weak or default passwords.
- Ransomware Detection: The honeypot identifies suspected ransomware-like behavior (e.g., file system activity or encryption-like activity) in the decoy environment.
- Traffic Anomaly Detection: The system analyzes the incoming traffic patterns for abnormal activity (e.g., excessive rates of failed logins or abnormal request rates).
- Known Attack Signature Matching: It is associated with known attack signature databases, which detect and categorize known threats.

Step 3:Threat Analysis and Logging Module

- Real-Time Attack Logging: The system logs attempts at attack, including IP addresses, time stamps, attack patterns, and payloads.
- Behavioral Profiling: Recognizes attacker behavior in the form of prevalent attack patterns.
- Interaction Metrics: Monitors how attackers interact with the honeypot services (e.g., commands, exploitation attempts).
- Dynamic Logs: Real-time logging allows for instant threat analysis.

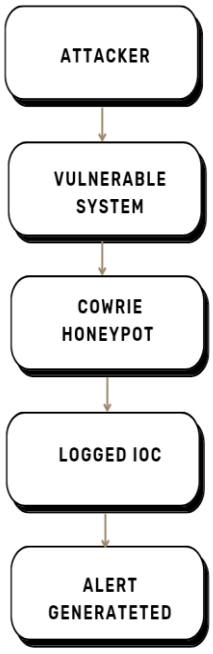
Step 4: Feedback Generation Module

- Real-Time Threat Detection: The system detects suspicious behavior in real-time, such as brute-force login attempts, possible ransomware behavior, and unusual interactions.
- Personalized Feedback: The system gives feedback based on the level and type of threats detected, with actionable feedback for administrators.
- Detailed Threat Reports: Once an attack is identified, the system generates detailed reports summarizing the source, technique, and potential impact on the honeypot of the attack.
- Alert System: Notifies administrators or security personnel through multiple channels (e.g., email, SMS) when there are critical threats.

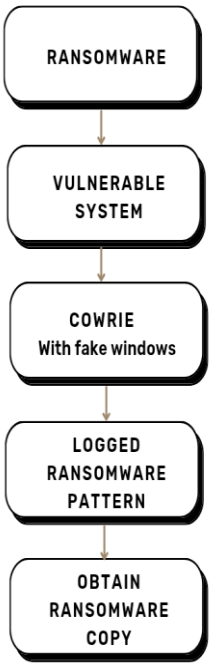
Step 5: Threat Analysis and Security Insights Module

- The system processes gathered attack data to determine attacker behavior trends.
- Examines repeated attack patterns, login attempts and command sequences utilized by attackers.
- Gives information about frequently utilized credentials, sources of attack, and methods of attack seen in the honeypot.
- Identifies possible threat actors, botnet activity, and new attack methods by comparing gathered attack data with known threat intelligence feeds.

Flow-Chart:



SSH -BRUTE FORCE



RANSOMWARE

IV. RESULTS

This work assesses the "Targeted Honeypot Deployment for SSH Brute-Force Attacks and Ransomware Analysis," which seeks to track and analyze unauthorized access attempts in real-time. Developed with Cowrie and combined with security logging software, the system offers an interactive and security layer while ensuring comprehensive attack monitoring. The tool uses log-based assessments to analyze attack behavior, monitoring. As attacks are made, logs are dynamically updated, providing real-time data.

COWRIE AND SSH BRUTE -FORCE

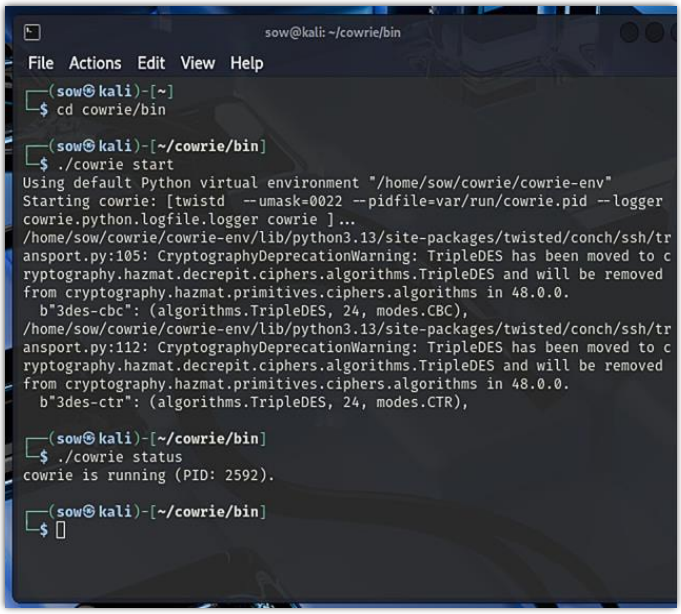


Figure 1: Cowrie-Setup

The Cowrie honeypot was successfully launched and confirmed to be active, showing the status message "Cowrie is running" and the process ID (PID) 2592. This confirmed that the honeypot was waiting for SSH connections and recording unauthorized access attempts. It was used as a decoy system, designed to capture attacker activity and study patterns of intrusion. The setup enabled detailed monitoring of login attempts, command execution, and session interaction in the simulated environment.

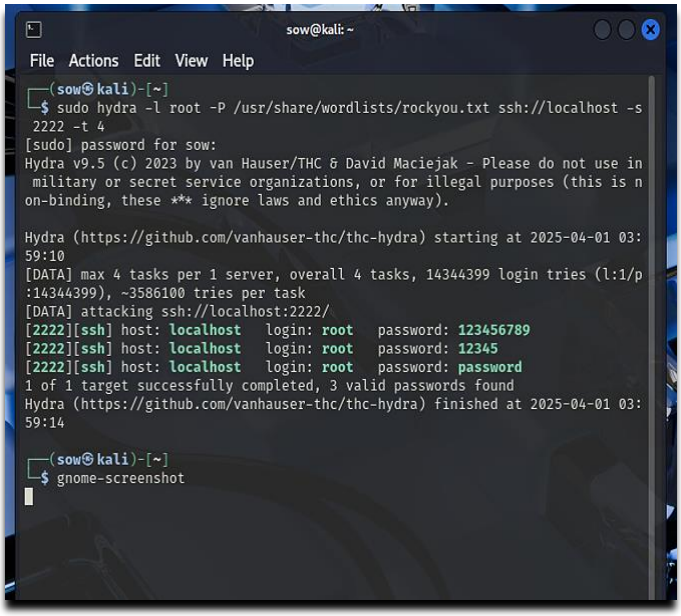


Figure 2: SSH Brute -Force simulation

To evaluate its effectiveness, a brute-force attack simulation was conducted using Hydra, a widely used password-cracking tool. The command sudo hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://localhost -s 2222 -t 4 was executed, targeting the honeypot on port 2222. The attack generated four login attempts, with the username “root” being used in each case, and the passwords being selected from a predefined wordlist.

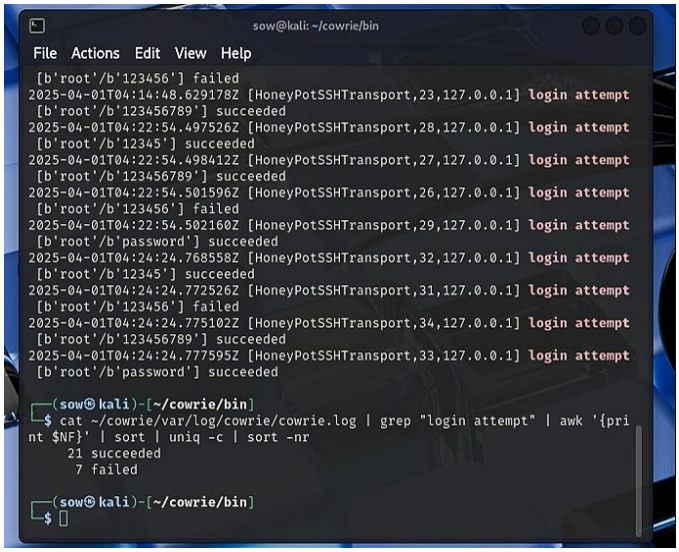


Figure 3: Login Attempt Details

Log analysis identified 23 successful and 7 unsuccessful logins, showing evidence of credential reuse and top choices for password selection used by attackers. More detailed analysis shows the overall analysis of attacker activity, including input commands, login attempts, and session information. The log information is instrumental in establishing attacker tactics and possible security vulnerabilities.

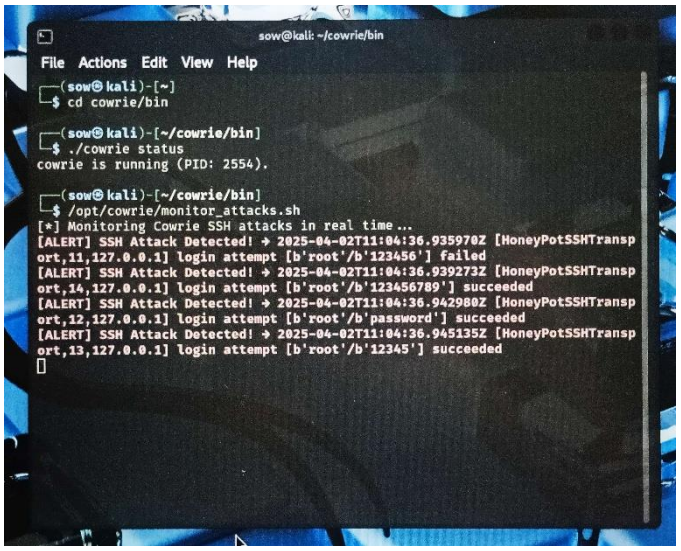


Figure 4: Real – Time Monitoring

To efficiently monitor and analyze real-time SSH attack attempts on the Cowrie honeypot, a real-time monitoring script (monitor_attacks.sh) was utilized. The script is located at /opt/cowrie/ and offers real-time monitoring of unauthorized login attempts, successful break-ins, and attacker activity on the honeypot system. Through the running of the script, administrators are able to monitor live logs of SSH activity, including brute-force attacks, login credentials utilized, and attacker commands**.**

RANSOMWARE CONFIGURATION

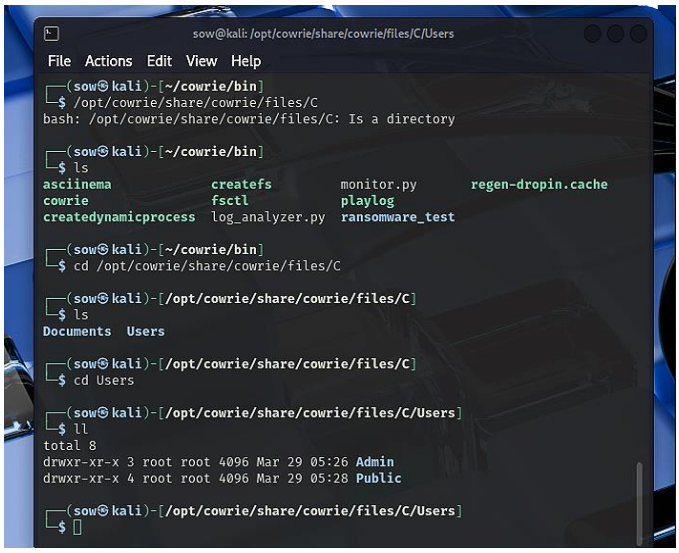


Figure 5 : Fake File system

Cowrie-emulated Windows-like file system for ransomware analysis. The directory hierarchy (C/Documents, C/Users/Admin, C/Users/Public) emulated is a real system to entice ransomware and monitor behavior. Monitoring of file interactions, encryption attempts, and access patterns aids ransomware execution analysis in a controlled environment. The ll command displays directory permissions, ownership (root), and timestamps, allowing managed access for forensic analysis and creating effective mitigation strategies.

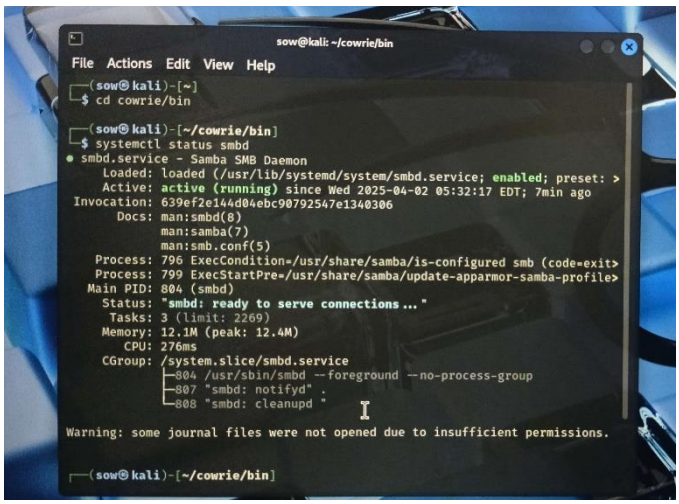


Figure 6 : Ransomware Configuration

The setup of SMB (Server Message Block) service via Samba (smbd) in Kali Linux, presumably for ransomware testing. The command systemctl status smbd checks that the smbd.service is running and active. Samba is employed for file sharing in Windows systems, so it is a popular target for ransomware, which encrypts network shared files. By activating SMB, the configuration simulates a vulnerable system, enabling monitoring of ransomware spread across network shares**.**

Findings:

The research proves the efficacy and effectiveness of the Targeted Honeypot Deployment for SSH Brute-Force Attacks and Ransomware Analysis in detecting and counteracting unauthorized attempts at access. Created with Cowrie, the system is efficient in monitoring and analyzing attack patterns while offering real-time information.

Effectiveness in Attack Detection:

The system effectively detected SSH brute force attacks, tracking attacker behavior and monitoring credential reuse. As the attack data piled up, trends were identified, helping to decipher attacker methods. The real-time monitoring of logs gave rise to actionable information, enhancing detection efficiency over time.

Security Insights and Threat Analysis:

The system recorded several attack vectors, such as repeated attempts to log in, bot based brute-force attacks, and unauthorized attempts. Analysis indicated that specific IP addresses and credentials were used multiple times, suggesting coordinated attacks. Such information can be useful in integrating threat intelligence in the future.

System Performance:

In spite of managing an increasing number of attack attempts, the Cowrie honeypot performed optimally, recording real-time attack data with no considerable loss of performance. The system handled a huge quantity of logs and ensured negligible overhead, thereby ensuring scalability in wider deployments effectiveness.

V. DISCUSSION

The results of this study indicate that the Targeted Honeypot Deployment for SSH Brute-Force Attacks and Ransomware Analysis, using Cowrie, effectively improves cybersecurity through real-time monitoring and attack analysis. Through the capture of detailed logs of unauthorized SSH login attempts, the system provides useful information regarding attacker behavior, frequently exploited credentials, and brute force methods.

The findings demonstrate that the honeypot was able to capture and analyze SSH brute force attacks successfully, capturing essential information such as source IP addresses, credentials attempted, and frequency of attack. Over a period of time, patterns could be seen where automated attack scripts and bot-powered credential stuffing attacks were present. These findings highlight the need for tracking login attempts in real-life situations since attackers tend to recycle credentials and hit weak authentication targets.

In addition, the system proved the efficiency of a honeypot in acquiring real-world attack information, making the logs gathered truly indicative of brute-force attack patterns and ransomware activity. Based on these logs, security teams can recognize attack patterns, evaluate unauthorized access attempts impact, and enhance mitigation techniques. Moreover, the system's vulnerability to simulating an attacked SSH environment was useful in misleading attackers, gaining more insights into attackers' tactics without compromising the actual system.

A. STUDY CONSTRAINTS AND RAMIFICATIONS

This study has a number of limitations that are to be taken into consideration. The study was carried out under a controlled setup, concentrating on a specific honeypot deployment for the detection of SSH brute-force attacks and the analysis of ransomware. Although the honeypot successfully captured attempts to attack, actual attack patterns will be different in various industries and networks. The study did not consider evasions that sophisticated attackers may use, which might restrict the system from being able to detect all possible threats.

Another shortcoming is the use of predefined logging and analysis techniques. Although they were useful in detecting unauthorized access attempts and frequent attack patterns, they were fixed and did not dynamically update themselves to counter new and evolving threats. Future deployments can be made more adaptable to evolving cyber threats using real-time threat intelligence feeds or machine learning-powered anomaly detection.

In addition, the research was concentrated mainly on monitoring attacks and data gathering, and not on the deployment of active countermeasures like automated IP blocking, rate limiting, or backend security hardening. Although these aspects were taken into account for future enhancement, they were not included in the present deployment. Future work could investigate the effect of incorporating automated response mechanisms and more in-depth forensic analysis to enhance the honeypot's contribution to proactive cybersecurity defense.

B. PROSPECTS FOR FUTURE RESEARCH:

Subsequent research can prioritize resolving the highlighted limitations and increasing the scope of SSH brute-force attack detection and ransomware examination in honeypot implementations. An important aspect of enhancement lies in integrating honeypots into enterprise security infrastructure, cloud environments, and IoT ecosystems to conduct a more in-depth analysis of attack patterns over diverse network setups.

Future honeypot designs might include real-time threat feeds and machine learning-based anomaly detection to further enable the system to detect new patterns of attack it has not previously seen. This would enable the honeypot to dynamically evolve to counter emerging threats instead of depending on static attack signatures.

Another key area is the automation of defensive countermeasures, including smart IP blocking, rate limiting, and integration with security information and event management (SIEM) systems. By automating response actions, the honeypot would be actively preventing attacks instead of acting as a passive monitoring tool.

Also, studies on honeypot deception methods—e.g., imitating actual systems more realistically to attract attackers—may enhance the performance of the honeypot. Using sandboxed ransomware execution environments for controlled analysis of malware behavior could also give further insights into ransomware infection. Lastly future research may investigate the psychological and behavioral dimensions of attackers engaging with the honeypot, examining how various honeypot settings affect attacker behavior which helps in the development of more effective cyber deception techniques .

VI. CONCLUSION

Most organizations and businesses have been fighting to detect and prevent SSH brute-force attacks and ransomware threats, since typical security mechanisms have failed to accurately log and examine attacker actions. Our research illustrates that using a focused honeypot with Cowrie gives one great information regarding attacker TTPs, thus allowing security professionals to make enhanced defensive tactics. The use of real-time monitoring enabled more active identification of attack patterns than in static log analysis.The results indicate that honeypots are an efficient decoy mechanism, enticing attackers into a sandboxed environment where their operation can be observed without putting true systems at risk. Through the trapping of brute-force efforts and SSH session activity, the honeypot assists in the determination of frequently exploited credentials, attack automation modalities, and prospective

IOCs. This methodology was considerably more effective than traditional log-based security analysis in interpreting actual attack behavior.The backend system provided the honeypot with the capability to function optimally, providing real-time attack logging and event tracking regardless of attack volumes. It could be further improved with future additions of threat intelligence feeds, automated blocking of IP addresses, and security event correlation software to better stop repeated attacks and help security administrators tune access control policies.

In conclusion, the SSH brute-force attack and ransomware analysis honeypot effectively enhances adversary behavior visibility and attacker profiling, even offering real-time insight into adversary action. It helps in strengthening the cybersecurity defenses of small to medium-sized organization.

VI. REFERENCES

1. Veena, K., M, M. T., Meena, K., Rajalakshmi, D., & C, H. (2023). *An Advanced Intrusion Detection Solution for Networks based on Honeypot Servers*. 1217–1222. https://doi.org/10.1109/icict57646.2023.10134511

2. Kamarudin Shah, M. F., Abdul Samad, A., A Ghaleb, F., & Md-Arshad, M. (2023). Comparing FTP and SSH Password Brute Force Attack Detection using k-Nearest Neighbour (k-NN) and Decision Tree in Cloud Computing. *International Journal of Innovative Computing*, *13*(1), 29–35. https://doi.org/10.11113/ijic.v13n1.386

3. Salamatian, S., Huleihel, W., Cohen, A., Medard, M., & Beirami, A. (2019). Why Botnets Work: Distributed Brute-Force Attacks Need No Synchronization. *IEEE Transactions on Information Forensics and Security*, *14*(9), 2288–2299. https://doi.org/10.1109/tifs.2019.2895955

4. Zhang, S., Xie, X., & Xu, Y. (2020). A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity. *IEEE Access*, *8*, 128250–128263. https://doi.org/10.1109/access.2020.3008433

5. Fan, W., Smith-Creasey, M., Fernandez, D., & Du, Z. (2019). HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design. *IEEE Journal on Selected Areas in Communications*, *37*(3), 683–697. https://doi.org/10.1109/jsac.2019.2894307

6. G. A. Jude Saskara, I. K. R. Arthana and P. B. Megawanta, "Simulation and Performance Testing of the Ganesha Honeypot System (GHOST) for SSH Security," *2023 1st International Conference on Advanced Engineering and Technologies (ICONNIC)*, Kediri, Indonesia, 2023, https://doi.org/10.1109/ICONNIC59854.2023.10467574

7. S. Mehta, D. Pawade, Y. Nayyar, I. Siddavatam, A. Tiwart and A. Dalvi, "Cowrie Honeypot Data Analysis and Predicting the Directory Traverser Pattern during the Attack," *2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, Chennai, India, 2021. https://doi.org/10.1109/ICSES52305.2021.9633881

8. V. -I. Năstase, M. -E. Mihăilescu, S. Weisz, L. V. Dagilis, D. Mihai and M. Carabas, "Cowrie SSH Honeypot: Architecture, Improvements and Data Visualization," *2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, Romania, 2024, https://doi.org/10.1109/RoEduNet64292.2024.10722609

9. M. Başer, E. Y. Güven and M. A. Aydın, "SSH and Telnet Protocols Attack Analysis Using Honeypot Technique: Analysis of SSH AND TELNET Honeypot," *2021 6th International Conference on Computer Science and Engineering (UBMK)*, Ankara, Turkey, 2021. https://doi.org/10.1109/UBMK52708.2021.9558948

10. K. Khaliq, N. Z. Ab Rahim, K. Hamid, M. Ibrar, U. Ahmad and M.U. Ullah,"Ransomware Attacks: Tools and Techniques for Detection," *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 2024. https://doi.org/10.1109/ICCR61006.2024.10532926

11. Roger A. Grimes, "Detecting Ransomware," in *Ransomware Protection Playbook* , Wiley, 2022 https://doi.org/10.1002/9781394177455

12. N. A. Malik *et al*., "Behavior and Characteristics of Ransomware - A Survey," *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 2024 https://doi.org/10.1109/ICCR61006.2024.10532983