IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, November 2025
Impact Factor: 7.67

# Analyzing Attacker Behaviour Using Honeypot and Log Analysis

**Yash Rajput[1], Krutika Pawar[2], Siddhika Salunke[3], Aarti Sahane[4]**
Students, Department of Computer Engineering[1,2,3,4]
Matoshri College of Engineering & Research Centre, Nashik, Maharashtra, India

**Abstract:** *Cyber threats have become increasingly sophisticated, with attackers continuously exploiting vulnerabilities in online systems. Understanding their behaviour and attack patterns is vital for designing proactive defense strategies. This research focuses on analyzing attacker behaviour through a medium-interaction honeypot named Cowrie, which emulates vulnerable SSH and Telnet services to attract attackers. The honeypot captures comprehensive logs of login attempts, executed commands, and session data. These logs are then processed through a Python-based log analyzer that extracts meaningful insights, such as the frequency of attacks, commonly used credentials, and origin IPs. The system is containerized using Docker for isolation and tested using Hydra, a brute-force tool from Kali Linux, to simulate attacks safely. Visualization tools like Matplotlib and Pandas are used to identify temporal and behavioural attack trends. The findings highlight how honeypots can effectively collect threat intelligence and aid in the development of adaptive cybersecurity systems.*

**Keywords**: Honeypot, Cybersecurity, Cowrie, Log Analysis, Docker, Hydra, Python, Threat Intelligence


DOI: 10.48175/IJARSCT-29620