Cyber Threat Intelligence Honeypot Project Report

Introduction

This project demonstrates the setup and execution of a Cyber Threat Intelligence Honeypot using the Cowrie SSH/Telnet honeypot on Kali Linux. The aim was to simulate real-world brute-force attacks, log attacker behavior, and analyze the collected data for patterns.

Objectives

- Deploy a Cowrie honeypot to capture attacker activities.
- Simulate brute-force SSH attacks using Hydra.
- Collect and parse logs to extract attacker IPs, usernames, and passwords.
- Visualize quick statistics for better insights.
- Showcase the project on GitHub with professional documentation.

Methodology

1. Installed dependencies and created a dedicated 'cowrie' user.
2. Cloned and configured the Cowrie honeypot.
3. Redirected SSH traffic to Cowrie by setting listen_port = 22.
4. Generated attacks using Hydra from a controlled environment.
5. Parsed logs using Python scripts to extract key insights.
6. Created quick statistics output (Top attacker IPs, Top attempted passwords).

Results

- Honeypot successfully captured SSH login attempts.
- Attacker IP (192.168.1.**) was logged with multiple failed and successful login attempts.
- Top attempted passwords included '12345', '123456', 'password', etc.
- Quick statistics provided clear summaries of attack patterns.

Screenshots

The following screenshots were taken as evidence:

- Starting cowrie.png: Cowrie honeypot running successfully.

- Capturing traffic attacked using hydra.png: Logs showing captured brute-force attempts.
- Quickstatus.png: Parser script displaying top IPs and passwords.

Challenges Faced

- Permission issues when accessing log files as the wrong user.
- Python library conflicts (pandas + numpy) caused visualization errors.
- Resolved by using a simplified quick_stats script.

Conclusion

The project successfully demonstrated the use of a honeypot for cyber threat intelligence. Cowrie captured attacker behavior, while Python scripts allowed quick analysis of attack trends.

This project can be extended by integrating visualization dashboards or automated blocking mechanisms (e.g., Fail2Ban).

References

- Cowrie Honeypot: https://github.com/cowrie/cowrie
- THC Hydra: https://github.com/vanhauser-thc/thc-hydra
- Kali Linux Documentation