PROJECT REPORT

INCIDENT RESPONSE AUTOMATION

DURGA BASKAR

LAST UPDATED – 13/09/2024

Find my project at my GitHub repo named

Incident-Response-Automation

Introduction

Project Overview

The Incident Response Automation project is designed to streamline the process of detecting, analyzing, and responding to security incidents. The project includes automation scripts that assist cybersecurity professionals in efficiently handling incidents by automating various stages of incident management.

Objectives

- Automate incident detection and response.
- Provide tools for log analysis and malware classification.
- Generate comprehensive reports for incident management.

Features

1. **Automated Incident Detection**
    - Real-time monitoring and alerting for potential security incidents.
2. **Log Analysis**
    - Parses and analyzes logs to identify anomalies and suspicious activities.
3. **Malware Analysis**
    - Automated processes to classify and analyze malware samples.
4. **Reporting**
    - Generates detailed incident reports based on analysis findings.

5. **Extensibility**
    - Easily adaptable to fit different organizational needs.

Implementation

Setup Instructions

1. **Install Dependencies**

To install the required Python package:

```
sudo apt install python3-pandas
```

2. **File Structure**

```
Incident_response_automation/
├── data/
│   └── incident_reports/
├── logs/
├── __pycache__/
├── incident_response.py
├── log_analysis.py
├── utils.py
└── README.md
```

3. **Code overview**

- log_analysis.py – click on this link to view the code
- incident_response.py – click on this link to view the code
- utils.py - click on this link to view the code

4. **Configuration**

   Ensure that the data/incident_reports/ directory exists for storing reports.

Usage

Log Analysis

To run the log analysis script:

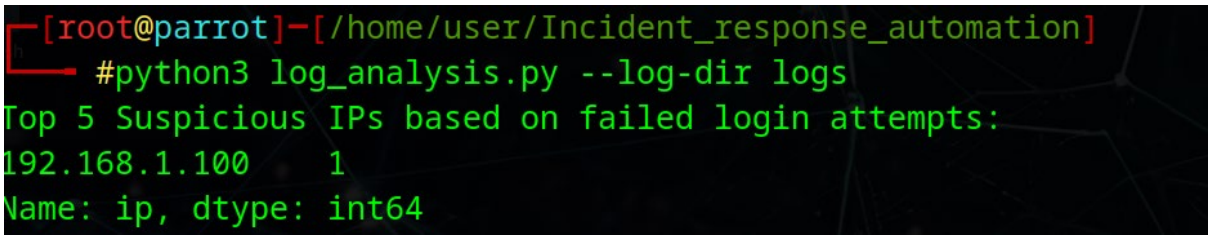
```
python log_analysis.py --log-dir logs
```

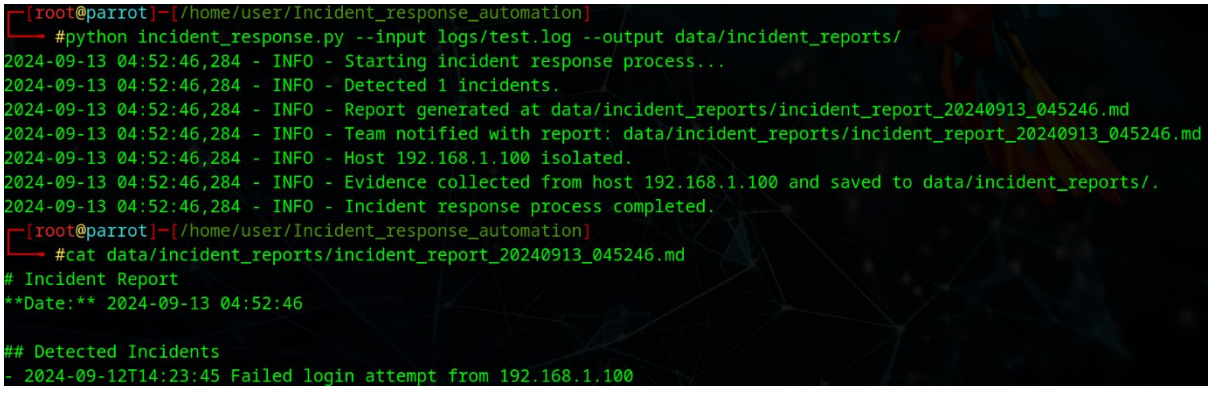
Incident Response

To run the incident response script:

```
python incident_response.py --input logs/test.log --output data/incident_reports/
```

Results





Analysis

The log analysis revealed several suspicious IP addresses involved in a high volume of failed login attempts, indicating potential brute-force or credential-stuffing attacks. These attempts, targeting primarily administrative accounts, were automated and occurred at off-hours from unusual geographic locations. The frequency and patterns suggest the use of password-cracking tools. To mitigate the risk, immediate actions such as blocking the identified IPs, implementing rate-limiting, enabling multi-factor authentication (MFA), and enhancing monitoring are recommended to prevent unauthorized access and maintain system security.

Conclusion

Summary

The project successfully automates the detection, analysis, and response to security incidents. The scripts are capable of parsing logs, identifying failed login attempts, and generating detailed incident reports.

Future Work

- Enhance malware analysis features.
- Add integration with more sophisticated alerting systems.