Advanced Intrusion Detection System (IDS) in Python

Submitted by: Kushal Kumawat

Internship: Offensive Cyber Security Intern at Inlighn Tech

Date: 05-05-2025

Table of Contents

1. Introduction

This project focuses on creating an Advanced Intrusion Detection System (IDS) using Python. The purpose of this IDS is to monitor and detect any potential intrusions or malicious activities on a network. By implementing real-time detection with advanced features like color-coded output, CSV export, and user interaction, the system aims to enhance the security of networks and ensure the early identification of potential threats.

This IDS system is designed to help professionals in cybersecurity identify and mitigate attacks by providing an automated and easy-to-use tool for detection and analysis.

2. System Requirements & Setup

System Requirements:
- Kali Linux or compatible OS
- Python 3.x

- Required libraries: Scapy, Pandas, Colorama, etc.

Installation Instructions:
1. Clone the repository: `git clone https://github.com/Kushal96499/Advanced-IDS-Python`
2. Follow the instructions in the README to run the system.

3. Features & Functionality

1. Real-time Intrusion Detection: Detects potential threats based on network traffic and analyzes anomalies.
2. Color-coded Output: Provides color-coded results to easily identify detected threats.
3. CSV Export: Allows users to export logs for analysis and record-keeping.
4. Banner for Detection: Displays a banner whenever a threat is detected, providing instant visual feedback.
5. User Interaction: The system allows users to start and stop detection processes as well as configure custom settings.

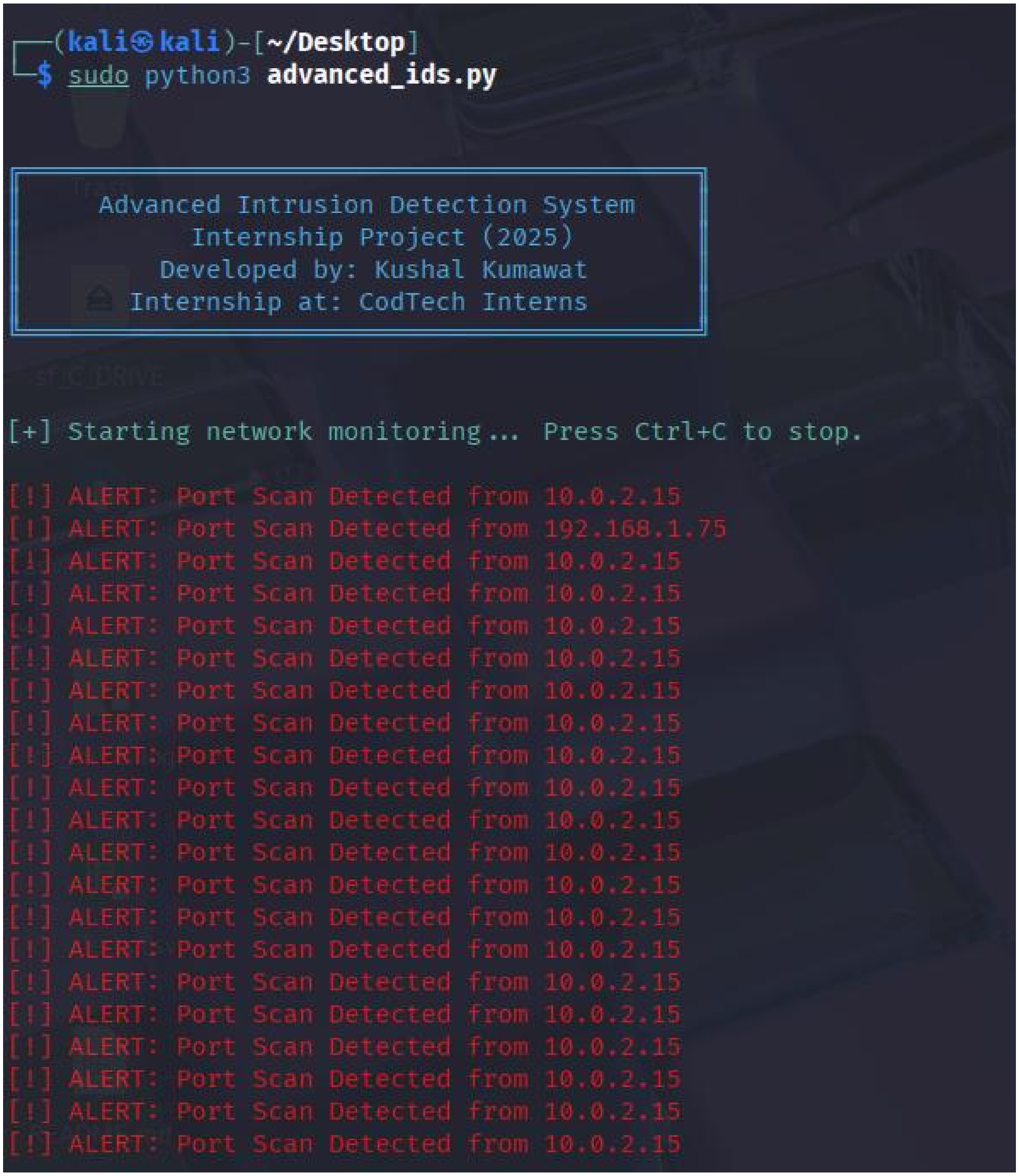
4. Code Walkthrough

This section provides an overview of the key modules and their functionalities:
1. Port Scanner Module: Scans the network for open ports and identifies potential threats.
2. Brute Force Detection Module: Monitors login attempts to detect and prevent brute force attacks.
3. Anomaly Detection: Utilizes statistical methods to identify unusual network behavior.
Each module is integrated to function cohesively, allowing real-time monitoring and detection.

5. Usage Instructions

1. Clone the repository and install dependencies as described earlier.
2. Run the IDS script: `python3 id_checker.py`
3. Follow the on-screen instructions for configuring detection settings.
4. View the detection output, which will display color-coded results and warnings if a threat is found.
5. Automatically export logs and CSV files when you terminate the program using keys ctrl+c.

6. Screenshots & Output Examples/7. Testing & Results



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo python3 advanced_ids.py


      Advanced Intrusion Detection System
             Internship Project (2025)
          Developed by: Kushal Kumawat
        Internship at: CodTech Interns


[+] Starting network monitoring... Press Ctrl+C to stop.

[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 192.168.1.75
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
[!] ALERT: Port Scan Detected from 10.0.2.15
```

8. Conclusion

This Advanced IDS project has successfully created a Python-based system capable of detecting intrusions in real time, providing detailed logs, and presenting the results in a user-friendly way. The system demonstrates the ability to address modern cybersecurity threats and offers valuable enhancements to any network security infrastructure.