Network Intrusion Detection System

-Abarna S (21PC01)

Aparnaa T (21PC04)

Samyukthaa B (21PC28)

This Python script serves as a comprehensive Network Intrusion Detection System (NIDS) with a range of functionalities aimed at monitoring and safeguarding network security. The utilization of Scapy enables the analysis of incoming packets for potential threats and notable events. The script employs blacklisting and whitelisting mechanisms, designating certain IP addresses as potential risks or trusted sources, respectively.

The logging system is a pivotal component, recording events in a rotating log file (network\_intrusion\_detection.log). This log provides a valuable resource for post-event analysis and forensic examination of network activities.

The integration of email alerts enhances real-time response capabilities. When a potential intrusion is detected, the script sends email notifications via a Gmail SMTP server. This proactive approach ensures that relevant stakeholders are promptly informed, allowing for immediate attention to potential security threats.

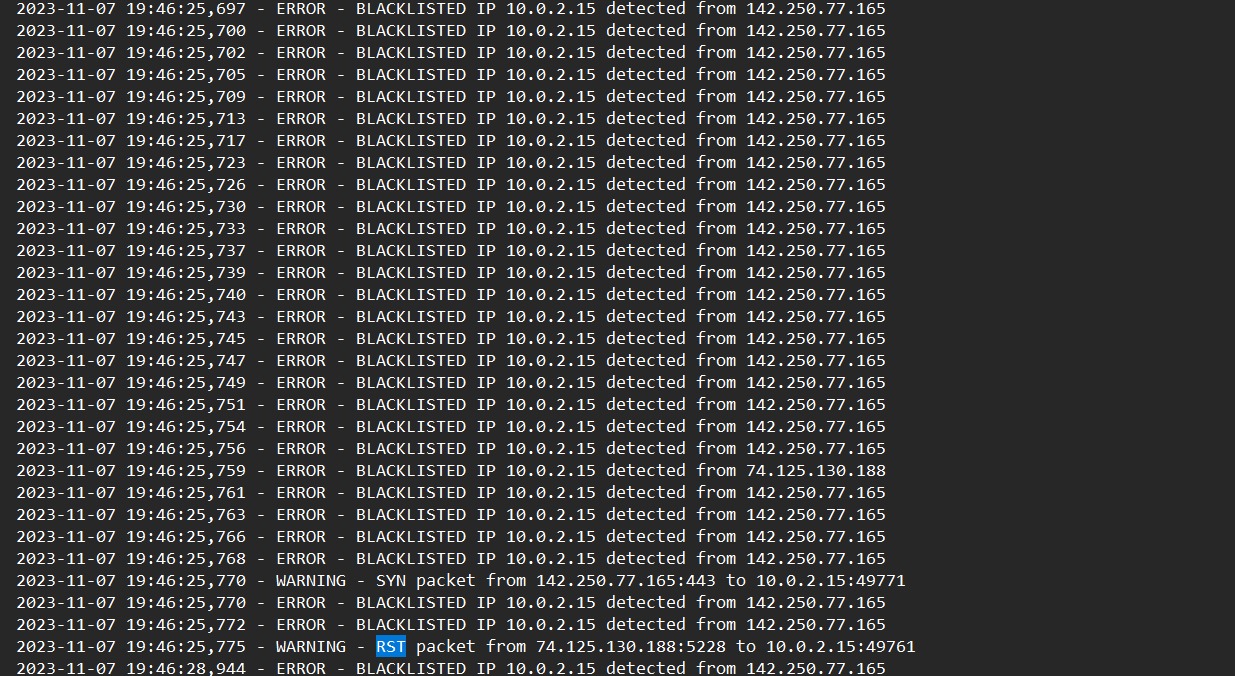
The core function, detect\_intrusions, scrutinizes each packet for IP and TCP layers. It identifies source and destination IPs, TCP flags, and packet content to determine potential security risks. If a source IP is in the blacklist, the script logs an error, sends an email alert, and takes action to block the IP by sending a TCP RST packet. Whitelisted IPs are logged as informational events, acknowledging trusted sources. Additionally, warnings are logged for SYN and RST packets, with corresponding email alerts for heightened visibility into network activities.

Furthermore, the script is designed to read network packets from a specified PCAP file (tcp.pcapng). This capability facilitates offline analysis of past network traffic, enabling users to retrospectively assess historical security events and patterns.

Output-



Log file-



Mail sent-

