IDS Python Script
DOCUMENTATION

SCRIPT FEATURES

Packet Capturing:

- Uses scapy.sniff to monitor live network traffic on a specified interface
- Captures and processes packets with a callback function.

Suspicious IP and Port Detection:

- Checks each packet for known malicious IPs or ports
- Logs activities to ids.log for future analysis

DDoS Detection:

- Counts the number of packets from each source IP
- Alerts if traffic exceeds a defined threshold

Extensibility:

- The script can be extended to include regex-based payload inspection or integrations with threat intelligence feeds

---

HOW TO USE

The script can be extended to include regex-based payload inspection or integrations with threat intelligence feeds

1. Install scapy: pip install scapy

2. Run the script with appropriate permissions (e.g., sudo to access the network interface)

3. Monitor the ids.log file for alerts: tail -f ids.log