**Here’s a user guide for your DDoS Monitoring Script:**

**User Guide: DDoS Monitoring Script**

**Overview:**

**This script is designed to monitor network traffic for potential DDoS attacks (Distributed Denial-of-Service). The system checks for abnormal packet traffic to a specific IP address (your machine) and triggers alerts when a source IP exceeds the predefined threshold for packet sending.**

**Key Features:**

* **Real-time Packet Monitoring: Uses scapy to monitor network packets.**
* **DDoS Detection: Triggers an alert if more than a certain number of packets are sent from a single IP address in a short time (threshold value is customizable).**
* **Automated Alerts: Sends Pushbullet notifications and logs attack details to a file.**
* **IP Information Lookup: Fetches detailed information about the attacking IP using the ipinfo.io API.**
* **Logging: Stores logs for detection, including attack source and additional IP information.**

**Pre-requisites:**

1. **Libraries & Tools:**
   * **Install the required Python libraries: scapy, requests, pushbullet.py.**
   * **pip install scapy requests pushbullet.py**
2. **API Keys:**
   * **Pushbullet API Key: Sign up at** [**Pushbullet**](https://www.pushbullet.com/) **and generate an API key.**
   * **ipinfo.io API Key: Create an account at** [**ipinfo.io**](https://ipinfo.io/) **and get your API key.**
3. **Network Access:**
   * **This script requires the ability to capture packets on the local machine using scapy's sniff() function.**
   * **Ensure that you have the necessary privileges to capture network traffic.**

**Script Configuration:**

1. **API Key for Pushbullet:**
   * **Replace YOUR\_Pushbullet\_Key in the script with your Pushbullet API key.**
2. **pb = Pushbullet("YOUR\_Pushbullet\_Key") # Replace with your token**
3. **API Key for ipinfo.io:**
   * **Replace Your\_IpInfo\_Key with your ipinfo.io API key to gather information about the attacking IP.**
4. **url = f'https://ipinfo.io/{ip}/json?token={API\_KEY}'**
5. **Packet Threshold:**
   * **The script considers an IP to be attacking when it sends more than dos\_threshold packets per second to your IP. You can adjust this value as required.**
6. **dos\_threshold = 10 # Threshold of packets per second from one source**
7. **Target IP:**
   * **The script monitors packets targeting your local machine’s IP. It automatically retrieves the local IP using socket.gethostbyname(socket.gethostname()).**

**How It Works:**

1. **Network Packet Sniffing: The script continuously listens for incoming packets using scapy's sniff() function. It filters out packets based on IP addresses, checking if the destination IP matches your local machine's IP.**
2. **DDoS Detection Logic:**
   * **For every incoming packet, the source IP is checked, and a packet counter for that IP is incremented.**
   * **If the source IP sends more than the defined number of packets (dos\_threshold) in one second, the system triggers a DDoS alert.**
3. **Notification: When an attack is detected:**
   * **A Pushbullet notification is sent to the configured device with details about the attack.**
   * **The source IP's information is fetched from ipinfo.io and logged to a file, including details like:**
     + **Location (City, Region, Country)**
     + **Org (Organization)**
     + **Hostname (If available)**
4. **Log Writing:**
   * **All detected attacks are logged into a file (DDos\_Monitor.log), along with the timestamp, attack details, and IP info.**
5. **Reset Mechanism:**
   * **Every 3 seconds, the script resets the packet count for all source IPs, clearing any previous data to avoid false positives.**

**Important Files:**

* **DDos\_Monitor.log: Contains logs of detected DDoS attempts with details like the source IP, attack timestamp, and additional info.**
* **targets.txt: Not needed for this script but could be adapted for use in a more extended version (to list target IPs for DDoS monitoring).**

**Running the Script:**

**To run the script, simply execute the following command:**

**python ddos\_monitor.py**

**The script will start sniffing the network traffic and will print logs to the console and also save them to the log file (DDos\_Monitor.log). Notifications will be sent when an attack is detected.**

**Sample Output:**

**Monitoring for DDoS attacks targeting 192.168.1.5...**

**[2023-04-21 14:32:21] Potential DDoS attack detected: 192.168.1.10 → 192.168.1.5 with packet count = 12**

**[2023-04-21 14:32:21] Attacking IP Info: {'IP': '192.168.1.10', 'Hostname': 'N/A', 'Location': 'Unknown, Unknown, Unknown', 'Org': 'Unknown', 'City': 'Unknown', 'Country': 'Unknown', 'Domain': 'N/A'}**

**Pushbullet alert sent.**

**Troubleshooting:**

* **If the script is unable to fetch IP info or send notifications, check your API keys for validity.**
* **Ensure that the network interface has permission for packet sniffing (admin/root privileges may be required).**

**This should help you get started with understanding and running your DDoS monitoring script.**