ARP Spoofing Detector - Explanation

---

1. Overview

This Python script **detects ARP spoofing attacks** and **sends alerts to Discord** when suspicious activity is found on the network.

---

2. Key Functions & How They Work

A. Fetching ARP Table

- Runs the command arp -a to list devices on the network.
- Retrieves **IP addresses**, **MAC addresses**, and **types** (static/dynamic).

B. Parsing ARP Table

- Extracts only **relevant entries** in the 192.168.1.x subnet.
- Filters out unnecessary information (headers, empty lines, etc.).

C. Detecting ARP Spoofing

- Checks if **one MAC address is linked to multiple IP addresses**.
- If found, it **flags it as suspicious**.

D. Formatting Data for Output

- Converts the ARP table into a **readable format** for logs and alerts.

E. Sending Alerts to Discord

- Uses a **Discord webhook** to send:
    - 🚨 **Spoofing Alerts** (if suspicious activity is found).
    - 🔍 **Normal Updates** (if the network is clear).

F. Continuous Monitoring

- Runs an **infinite loop** that:
    1. Fetches ARP data every 60 seconds.
    2. Checks for spoofing.
    3. Sends updates to Discord.

---

3. How It Detects ARP Spoofing

✓ If multiple IPs share **the same MAC address**, it triggers an alert.
✓ If one of these IPs is **the gateway (e.g., 192.168.1.1)**, the router might be spoofed.
✓ Sends an alert with **full details of the ARP table** to Discord.

---

4. Example Alert in Discord

🚨 **ALERT: ARP SPOOFING DETECTED!**
Suspicious IPs: 192.168.1.10, 192.168.1.20
Gateway IP: 192.168.1.1
Timestamp: 2025-03-08 14:30:00

```
IP Address      MAC Address          Type
-----------------------------------------------
192.168.1.1     aa-bb-cc-dd-ee-ff    dynamic
192.168.1.10    aa-bb-cc-dd-ee-ff    dynamic  <-- Spoofing
192.168.1.20    aa-bb-cc-dd-ee-ff    dynamic  <-- Spoofing
```

---

5. Summary

🔥 **Detects ARP spoofing attacks in real-time.**
💡 **Sends alerts to Discord for quick response.**
🚀 **Can be extended to block attackers using firewall rules.**