| S.No | Problem Statement ID | Problem Statement Name | Domain |
|---|---|---|---|
| 3 | CT-DFIR - 03 | Network Forensics | DFIR |

## Description :

This project involves building a tool to analyze and monitor network connections, focusing on detecting hidden or masked activities behind public IP addresses. Criminals or insider threat actors often disguise their true identity by using public IPs or masking techniques, making it challenging to trace their activities. The **PROBE Tool** will help identify and trace these hidden connections by analyzing IP, MAC, and packet data.

In its advanced stage, the tool will also have the ability to terminate malicious connection requests made by the threat actor, providing an active defense mechanism. This solution will be agentless, meaning it won't require installation on individual devices, and will focus on intrusion detection and network traffic monitoring.

**Objectives :**

1. **Prelims :**
    - Trace and identify hidden connections linked to a public or masked IP address.
    - Analyze network traffic to uncover behind-the-scenes connections using packet data and MAC addresses.
    - Provide visibility into all devices and connections in a network, including those attempting to mask their origin.
2. **Mains :**
    - Add a feature to terminate malicious connection requests from identified threat actors.
    - Enhance the tool to actively monitor and block suspicious movements in real-time.
3. **Automation and Efficiency :**
    - Build an agentless solution for easy deployment across networks.
    - Focus on creating an intuitive interface to visualize network traffic and suspicious connections.

**Expectations :**

1. **For Developers :**
    - Develop a tool that can analyze network traffic without installing software on individual devices.
    - Use techniques like packet inspection and MAC/IP tracking to trace connections.
    - Simulate insider threat scenarios to test the tool’s capabilities.
2. **For Security Teams:**
    - Provide a solution to detect and trace hidden connections linked to a public IP address.
    - Enable proactive measures to block or terminate malicious activities.
3. **For End Users:**
    - Offer a simple and easy-to-use interface for network monitoring.
    - Deliver clear insights about suspicious connections and movements.

**Expected Results:**

1. **Network Visibility:**
    - Detailed mapping of all devices and connections in the network.
    - Ability to trace connections hidden behind public or common IP addresses.
2. **Intrusion Detection:**
    - Identify and flag suspicious activities based on IP, MAC, and packet data analysis.
    - Detect insider threat actors trying to hide or mask their activities.
3. **Threat Prevention:**
    - Terminate malicious connection requests from identified threat actors in real-time.
    - Block suspicious movements before they can escalate into significant threats.
4. **Agentless Monitoring:**
    - Provide a lightweight solution that does not require installing agents on devices, making deployment easier and faster.