S.No	Problem Statement ID	Problem Statement Name	Domain
23	CT-OSINT - 05	Decoding Virtual Numbers	OSINT / Threat Intelligence

Description:

The **Virtual Number and VoIP Intelligence Tool** is designed to assist in tracing virtual numbers and Voice over Internet Protocol (VoIP) calls often used in cybercrimes like bullying, harassment, and fraud. Virtual numbers, which can originate from any country code (e.g., +1, +44), make it challenging to track perpetrators.

This tool decodes the IP and gathers basic information about VoIP calls, including SIP (Session Initiation Protocol) details. It provides intelligence on the origin of the virtual number, websites or platforms used, and basic user details, helping investigators gain insights into cybercriminal activities.

Objectives:

1. **Trace Virtual Numbers:**
   - Identify the origin and service provider of virtual numbers used in cybercrimes.
2. **VoIP Call Intelligence:**
   - Decode IP addresses associated with VoIP calls and analyze SIP trunking packets.
3. **Gather User Information:**
   - Extract and display basic details about the users operating virtual numbers and VoIP services.
4. **Domain Name Lookup:**
   - Integrate a lookup feature for identifying the domains and platforms involved.
5. **User-Friendly Interface:**
   - Provide an easy-to-use application or software for investigators to trace calls and gather intelligence quickly.

Expectations:

For Hackathon Participants:

1. **Develop a Prototype:**
   - Create a basic tool capable of tracing virtual numbers and decoding VoIP call details.
2. **Integrate SIP Analysis:**
   - Include packet detection for SIP trunking services and provide open port analysis.
3. **Design an Interface:**
   - Build an intuitive user interface to display results like call origin, IP address, and user details.
4. **Include Domain Lookup:**
   - Implement a feature to perform domain lookups for services linked to the virtual numbers.
5. **Focus on Automation:**
   - Automate data collection and analysis to simplify the investigation process.

For Law Enforcement Agencies (LEAs):

1. **Identify Call Origin:**
   - Trace the source of virtual numbers and VoIP calls used for cyberbullying or fraudulent activities.
2. **Track User Details:**
   - Retrieve details about users operating from specific platforms or domains.
3. **Simplify Investigations:**
   - Automate IP tracking, VoIP call analysis, and virtual number tracing for quicker case resolutions.
4. **Provide Actionable Intelligence:**
   - Deliver clear insights into the infrastructure and origin of the calls.
5. **Enhance Digital Forensics:**
   - Assist in building strong digital evidence for legal actions.

Expected Results:

1. **Virtual Number Tracing:**
   - Provide information about the country, platform, and user of virtual numbers.
2. **VoIP Call Decoding:**
   - Decode IPs, identify open ports, and extract SIP trunking details for calls.
3. **User Insights:**
   - Retrieve basic user details tied to the virtual number or VoIP call.
4. **Comprehensive Reports:**
   - Generate detailed reports of findings, including domain lookup results.
5. **Efficient Investigations:**
   - Save time by automating processes and simplifying technical analysis for investigators.