# **CTF Topic: Threatcrowd**

# **1. Introduction**

ThreatCrowd is an open-source threat intelligence tool that allows users to explore and analyse domains, IPs, and other indicators of compromise (IOCs) to understand the relationships and connections between them. This CTF challenge will help you get familiar with using ThreatCrowd for threat intelligence and analysis.

# **3. Scenario**

You are a cybersecurity analyst tasked with investigating a suspicious domain that has been flagged in your company's security logs. Your goal is to use ThreatCrowd to gather intelligence on this domain, uncover its associations, and determine if it poses any threat to your organization.

# **4. Process to Follow while Performing CTF**

Step 1: Visit the ThreatCrowd website:[**http://ci-www.threatcrowd.org/**](http://ci-www.threatcrowd.org/)

Step 2: Enter the suspicious domain into the search bar: [**www.google.com**](http://www.google.com)

Step 3: Analyze the results, including any related IP addresses, associated domains, and email addresses.

# 

# **5. Let's Begin The Challenge**

# **Question**

**Flag 1: What is the whois registrar name?**

**Answer: MARKMONITOR INC.**

**Flag Captured.**

**Flag 2: What is the subdomains of ip 66.249.80.100**

**Answer:** [**google-proxy-66-249-80-100.google.com**](http://ci-www.threatcrowd.org/domain.php?domain=google-proxy-66-249-80-100.google.com)

**Flag Captured**

# **Hint**

