## ****DNS Reputation Analysis Tool – Assignment****

### ****Project Overview****

The goal of this project is to develop a DNS traffic reputation analysis system capable of:

1. Re-playing DNS traffic from PCAP files.
2. Parsing DNS queries from the replayed traffic.
3. Performing high-throughput reputation lookups for unique domains.
4. Providing comprehensive monitoring, logging, and reporting.

### ****Assignment Tasks****

#### **1. Traffic Re-play Manager**

Develop a component to reliably re-play DNS traffic from PCAP files.

**Requirements:**

* Lifecycle management: start, monitor, and stop replay.
* Real-time statistics:
  + Packets sent
  + Errors encountered
  + Query rate (DNS queries per second)
* Graceful shutdown handling (e.g., Ctrl+C)

#### **2. Asynchronous Reputation Engine**

Implement a concurrent DNS reputation checker.

**Requirements:**

* Query the Reputation API for each extracted domain.
* Support high-concurrency lookups.
* Enforce per-request timeouts and retries.
* Implement caching with expiration for domain results.
* Ensure resilience: continue processing even if some lookups fail.
* Robust error handling.
* Configurable request rate (RPS) to control system load.

**API Details:**

GET https://microcks.gin.dev.securingsam.io/rest/Reputation+API/1.0.0/domain/ranking/{DOMAIN}

Header: Authorization: Token I\_am\_under\_stress\_when\_I\_test

**Example Response:**

{

"address": "google.com",

"reputation": 100,

"categories": ["general"]

}

**Scoring Classification example:**

* 0–60 → Untrusted
* 61–100 → Trusted

#### **3. Monitoring & Reporting**

Track and report runtime statistics continuously.

**Metrics to Collect:**

* Queries per second (QPS)
* Response time distribution (average, min, max)
* Request counts: total / succeeded / failed

**Shutdown Behavior:**

* On timeout or keyboard interrupt, print and save a final summary: Test is over! Reason: timeout / keyboard interrupt Total runtime: 38 seconds Requests total: 3210 Domains processed: 593 Average response time: 120 ms Max response time: 1.2 sec
* If timeout occurs before all domains are processed, terminate immediately.
* Ensure total runtime does not exceed the timeout plus a small buffer.

**Saved Results Format (CSV/JSON):**

* Domain
* Reputation score
* Classification (Trusted/Untrusted)
* Categories
* Query source (from PCAP)
* Response time

### ****Deliverables****

1. **Code**
   * Fully functional implementation of all components.
   * Organized as a structured Python project with clear module/package hierarchy.
2. **Documentation**
   * README.md including:
     + Project overview
     + Setup and installation instructions
     + Example usage
3. **GitHub Repository**
   * Upload the project to a **private** GitHub repository.