**TASK 2**

### Objective

To use **Maltego CE** for:

* Mapping the infrastructure of testphp.vulnweb.com.
* Identifying vulnerabilities like CVE-2023-44487 (HTTP/2 Rapid Reset attack).
* Extracting data such as email addresses, subdomains, and IP addresses.
* Analyzing gathered data to identify potential risks.

### Prerequisites

1. Install **Maltego CE**: Download it [here](https://www.maltego.com/" \t "C:\\Users\\PERFEC~1\\AppData\\Local\\Temp\\_new).
2. Create a Maltego account and log in to activate.
3. Ensure access to the internet for running transformations.
4. Permission from the target's owner (for ethical testing).

### Steps Performed

#### Step 1: Starting from the Domain Entity

1. Open **Maltego CE** and create a new graph.
2. Drag the **Domain (Internet Domain)** entity from the entity palette.
3. Rename the entity to testphp.vulnweb.com.

#### Step 2: Running Transformations on the Domain

1. Right-click the testphp.vulnweb.com entity and run:
   * **To IP Address [DNS]**: Resolves the domain to its IP address (44.288.249.3).
   * **To DNS Names**: Finds related subdomains, if any.
   * **To WHOIS Record**: Fetches registration details.
   * **To Email Addresses**: Extracts associated email addresses from public sources.
2. Results:
   * **IP Address**: 44.288.249.3.
   * **Email Addresses**: Extracted emails (e.g., admin@testphp.vulnweb.com).

#### Step 3: Analyzing the IP Address

1. Use the derived IP (44.288.249.3) and run:
   * **To CVE**: Matches known vulnerabilities (e.g., CVE-2023-44487).
   * **To Services and Ports [Shodan]**: Lists open ports and running services.
   * **To Web Technologies**: Identifies server software and technologies.

#### Step 4: Identifying Files and Media

1. From the domain, run:
   * **To Files [Public Internet]**: Retrieves linked files (e.g., test.php, .gif, .png).
   * **To Web Links**: Extracts publicly linked web pages and file directories.

#### Step 5: Investigating CVEs

1. On the CVE entity (e.g., CVE-2023-44487), review:
   * Associated software vulnerabilities and descriptions.
   * Applicability to the detected IP and services.

### Key Findings

* **Domain**: testphp.vulnweb.com.
* **Resolved IP**: 44.288.249.3.
* **Open Ports**: (from Shodan data):
  + Port 80 (HTTP).
  + Port 443 (HTTPS).
* **Email Addresses**:
  + admin@testphp.vulnweb.com
  + Other emails, if found.
* **Files and Media**:
  + test.php
  + .gif and .png images.
* **Relevant CVEs**:
  + **CVE-2023-44487** (HTTP/2 Rapid Reset attack).
  + Other CVEs related to the web server or software versions.

### Report Generation

While **Maltego CE** doesn't generate reports directly, you can:

1. Export the graph:
   * Go to **File > Export**.
   * Choose **Export as Image** for the graph or **Export Entities** for detailed entity data.
2. Create a manual report:
   * Use the exported graph and collected data to compile your findings.
   * Include:
     + **Summary**: Overview of the domain and IP findings.
     + **Infrastructure Details**: Subdomains, IPs, and services.
     + **Vulnerability Analysis**: CVEs and associated risks.
     + **Recommendations**: Steps to mitigate vulnerabilities.

### Example Report Outline

#### Title: Reconnaissance and Vulnerability Assessment of testphp.vulnweb.com

#### 1. **Introduction**

* Objective and scope of the reconnaissance.

#### 2. **Methodology**

* Steps taken in Maltego to map infrastructure and identify vulnerabilities.

#### 3. **Findings**

* **Domain**: testphp.vulnweb.com.
* **IP Address**: 44.288.249.3.
* **Open Ports**: Port 80 (HTTP), Port 443 (HTTPS).
* **Email Addresses**: admin@testphp.vulnweb.com.
* **Files and Media**: test.php, .gif images.
* **CVEs**:
  + **CVE-2023-44487**: Description and risks.
  + Other relevant CVEs based on software versions.

#### 4. **Recommendations**

* Apply patches for detected CVEs.
* Update server software and close unused ports.

#### 5. **Graphical Representation**

* Include the exported Maltego graph (hierarchically organized).

***Relevant Screen shots:***









