TITLE: CodTech IT Solutions Internship - Task Documentation: “Use Maltego GUI based tool and Gather information about the given target site

INTERN INFORMATION:

Name: Macha Bhagath

ID: COD5891

INTRODUCTION

Maltego GUI, a powerful tool for Cybersecurity and digital investigation, is discussed. Developed by Paterva, the user-friendly GUI helps users gather valuable information from various sources. Built on Transformations, it extracts data from OSINT platforms, databases, social media, and more. Maltego GUI enables efficient data analysis, visualization, and threat identification, aiding informed decisions and improved Cybersecurity. The text covers features, functionalities, use cases, and industries benefiting from its integration.

The tool helps visualize complex relationships between entities, uncovering hidden connections and patterns. Its key features include an extensive library of transforms for data extraction from various sources, such as OSINT and proprietary databases. The user-friendly interface and customizable workflow make it efficient and productive for both beginners and experts.

Implementation

- **Download and Install Maltego:**

  Visit the Paterva website and create an account to access the Maltego software.

- **Activate Your License:**

  After installation, launch the Maltego GUI tool. You will be prompted to activate your license. If you have purchased a license, enter the activation key provided in your account. If you are using the free version, select the appropriate option.

- **Understand Transforms and Entities:**

  Transforms are pre-configured actions that help extract specific types of data from various sources. Entities are the objects you analyze, such as individuals, organizations, websites, or IP addresses. To use transforms, drag and drop them onto the selected entity in the Graph View.

- **Explore Transform Libraries:**

  Maltego offers different transform libraries, including Open Source Intelligence (OSINT), Cybersecurity, and Digital Forensics. Explore these libraries to find the most suitable transforms for your investigations.

- **Configure and Customize the Workflow:**

  Maltego allows users to customize their workflow by adding or removing transforms, setting preferences, and configuring the tool according to their needs. You can create custom transforms or modify existing ones using the Maltego Transform Development Kit (TDK).

- **Analyze and Visualize Data:**

  As you apply transforms to entities, Maltego will gather and display the data in the Graph View. Visualize connections between entities to uncover hidden patterns and relationships.

- **Connect to Data Sources:**

  To gather information, connect Maltego to various data sources, such as OSINT repositories or proprietary databases. You can add data sources by configuring transforms or using the "Add Data Source" option in the Transform Panel

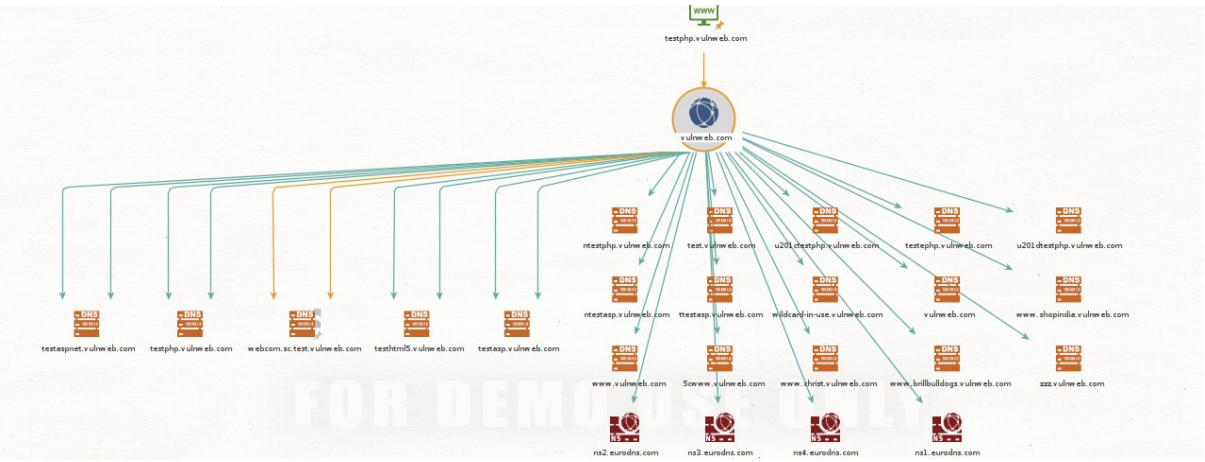
- **Export and Share Results:**

  Once you have completed your analysis, you can export the results in various formats, such as XML, CSV, or PDF. Additionally, you can share your work with others by exporting the entire Maltego project.

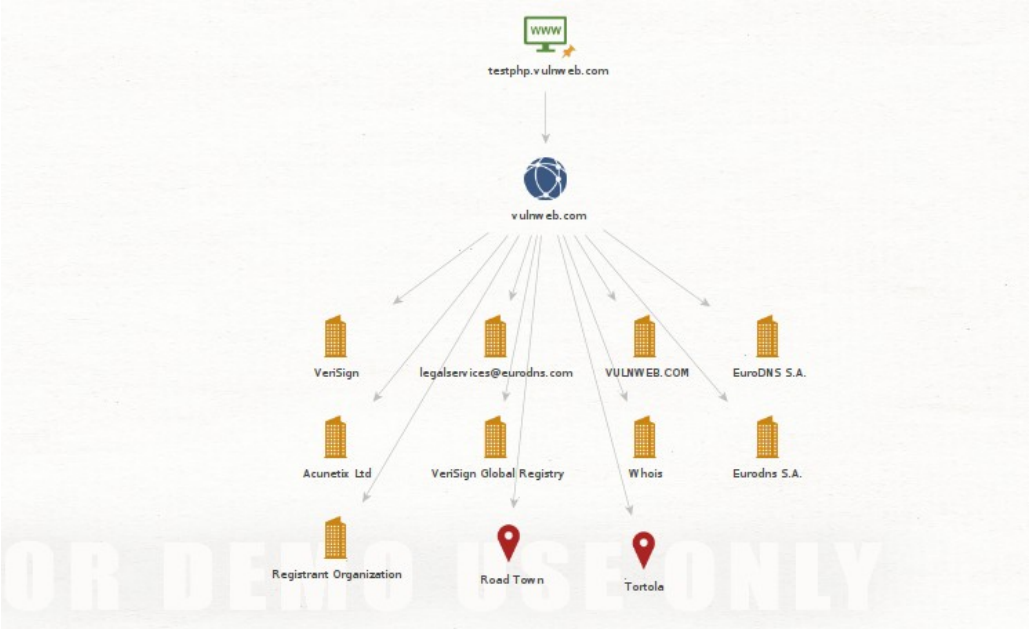
Workflow

- The target site http://testphp.vulnweb.com/ appears to be a web resource designed for educational purposes, specifically focused on web application security and vulnerability testing. The site contains various PHP scripts that intentionally exhibit different types of security weaknesses, such as SQL injection, command execution, and file inclusion.
- Launch the Maltego application and create a new graph in Maltego by clicking on the "+" icon in the top left corner.
- In the search bar, type "Website" and create a new Website entity.
- Paste the target site URL (http://testphp.vulnweb.com/) into the Website entity and now Right-click on the Website entity and select "Run Transforms.

- In the search bar, type "DNS" and select the "To Domain-DNS" transform. Run the transform.
- **DNS and NS Record (Transform Used: To DNS Name – Security Trails)**
  Now RIGHT-CLICK on Domain and In the search bar, type "DNS NAME" and select the "To DNS Name – Security Trails" transform. Run the transform.

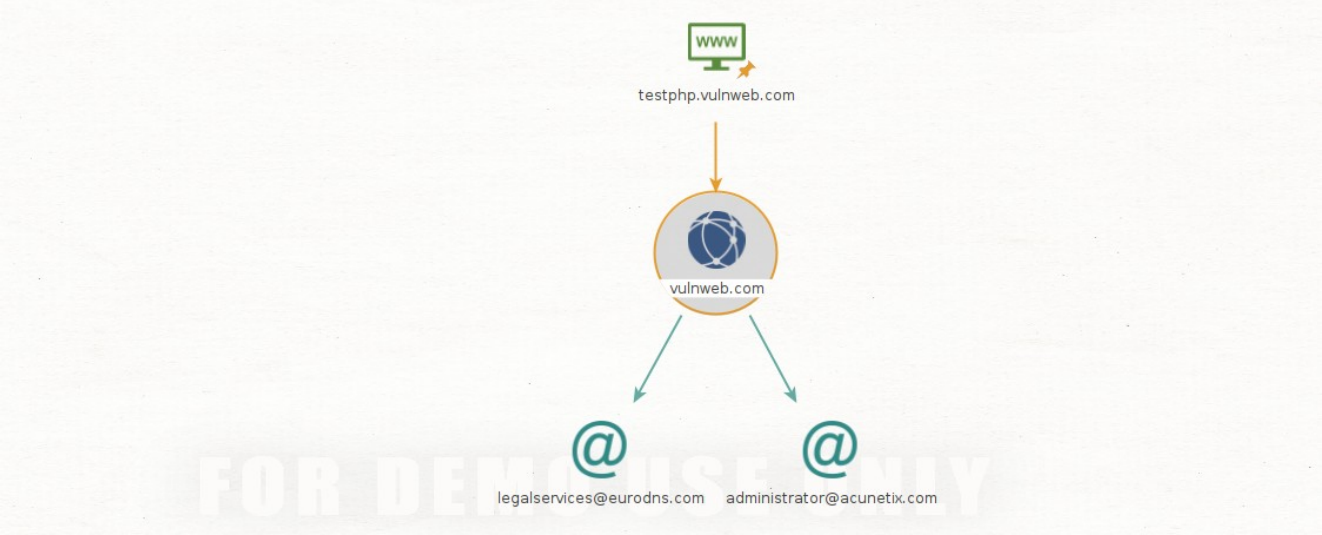


- **Companies and Locations (Transform Used: To Entites from WHOIS – IBM)**
  Now RIGHT-CLICK on Domain and In the search bar, type "WHOIS" and select the "To Entites from WHOIS – IBM Waston" transform. Run the transform.



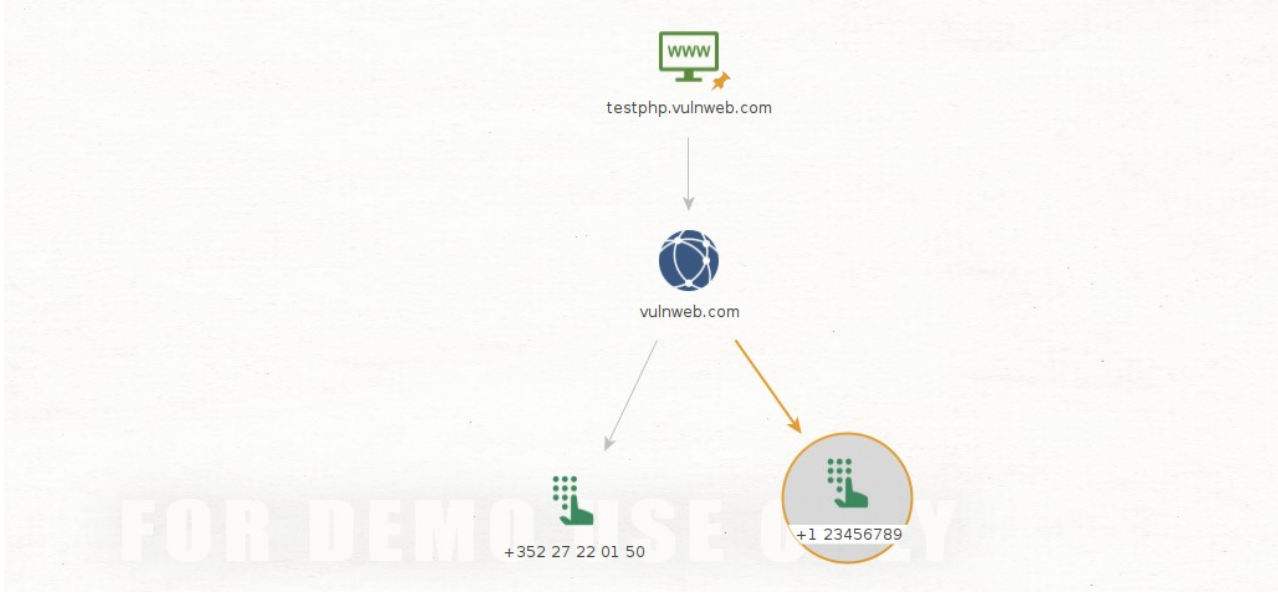
- **Email Address (Transform Used: To Email Address – from WHOIS info)**

  Now RIGHT-CLICK on Domain and In the search bar, type "WHOIS" and select the "To Email Address – from whois info" transform. Run the transform.



- **Phone Numbers (Transform Used: To phone Number – from WHOIS info)**

  Now RIGHT-CLICK on Domain and In the search bar, type "WHOIS" and select the "To Email Address – from whois info" transform. Run the transform.



Analyze the gathered information

This analysis aims to provide a structured overview of the extensive information gathered about a particular company. The data includes phone numbers, Gmail accounts, locations, associated companies, domain names, and DNS records. The significance of this information lies in understanding the company's infrastructure, communication channels, and possible relationships with other entities

Key Findings:

1. Contact Information:

The gathered data reveals various phone numbers and Gmail accounts associated with the company. This information is crucial for effective communication and maintaining relationships with clients, suppliers, and employees

2. Geographical Presence:

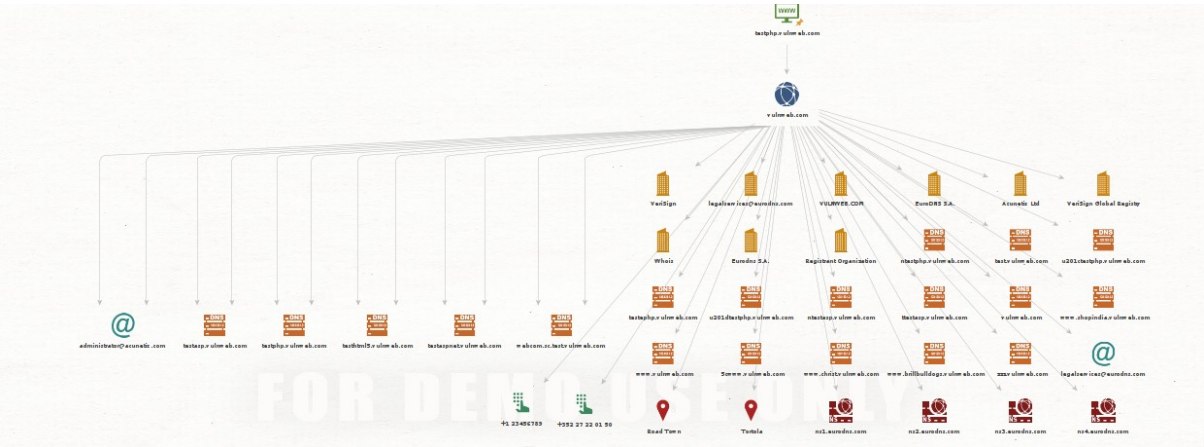
Multiple locations have been identified in connection with the company, suggesting a possible multinational presence or regional operations. This geographical spread may indicate the company's growth potential and its ability to serve diverse markets.

3. Domain Names and Websites:

Several domain names have been discovered, which may correspond to the company's websites or online properties. These websites could provide valuable insights into the company's products, services, and overall online presence.

4. DNS Records:

DNS records have been identified, which are essential for mapping domain names to IP addresses. This information can help in understanding the company's server infrastructure, website performance, and potential security measures in place.



CONCLUSION

In conclusion, the information gathered through the use of the Maltego GUI tool provides an extensive and intricate overview of a company, encompassing various aspects such as phone numbers, Gmail accounts, locations, associated companies, domain names, and DNS records. This wealth of data enables a comprehensive understanding of the organization, facilitating in-depth analysis and informed decision-making. As a result, the Maltego GUI tool remains a valuable asset for individuals and organizations seeking to explore and examine the complexities of companies in today's interconnected world.This data can be further utilized for Identifying threats, risks, Conducting vulnerability assessments and penetration testing