**TITLE: CodTech IT Solution Internship**

**TASK:** Use Maltego GUI based tool and Gather information about the given target site (<http://testphp.vulnweb.com/>)

**INTERN INFORMATION**

**Name: Himanshu Kumar**

**ID: ICOD7205**

**INTRODUCTION ABOUT MALTEGO GUI**

Maltego is a powerful data visualization and link analysis tool used in the field of cybersecurity, intelligence gathering, and law enforcement. Its graphical user interface (GUI) is designed to facilitate the exploration and visualization of complex relationships and connections between various entities, such as people, organizations, websites, and more. Some of the important features of the maltego GUI are as follows:

(a) Entity Palette: It provides different types of entities that can be used to gather information about your investigation. to select any entities, you have to drag that entity onto the workplace.

(b) Workplace: It Provides a place where we construct our investigation graph. Each and every graphs are easy to understand and visualize the relationship between them.

(c) Transforms: These are the actions that can be used to gather information about different categories like DNS, name server, email phone number, location etc.

Steps to install Maltego GUI:

Step 1: Visit the official website of maltego to get original Maltego Software.

Step 2: Register free for community edition with your email id and create strong password.

Step 3: Open the maltego application and login with the same email and password in community edition.

Now, Maltego GUI is fully ready to use and we can start our investigation.

**Understand transformation and entities:**

Transforms are pre-configured actions that help extract specific types odd data form various sources. Entities are the objects you analyse, such as individuals, organizations, websites, or IP addresses. To use transforms, drag and drop them onto the selected entity in the graph view.

**Transform Libraries:**

The different libraries that are being offered by maltego are Open-Source Intelligence (OSINT), Cybersecurity, Digital Forensics. And now we have to figure it out which libraries will be helpful for our investigation.

**Customizing and configure the workflow:**

By adding and removing transforms, Maltego allows users to customize their workflow as required by their needs. It also helps to create our own transforms or modify the existing transforms using Maltego Transform Development Kit.

**Analyse the Data:**

After applying the transforms to entities, Maltego gathers the information and display them in the form of graph in the workflow. It helps to visualize connections between entities to find relation between them.

**Exporting and Saving the Outputs:**

After applying the transform and completing the information gathering we have to save or export our result, it can be done in various format such as XML, CSV, or PDF. And we can also share those results with others by exporting the entire Maltego Project.

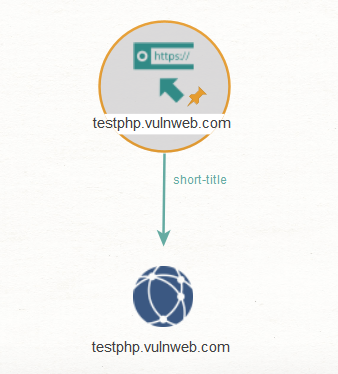
**Using the Maltego to gather information on the given target:**

1. First, we required a target from which we have to gather information, in my case the target is <http://testphp.vulnweb.com/> , this site is being designed for educational purpose. It helps us to understand that how a developer errors and bad configuration may lead to someone to break into our websites.
2. We are going to use Maltego to gather information, we will launch the maltego and start a new graph to start our work.
3. In the entities palette section we have to search for URL, because we have the URL of our target website.
4. Drag and drop the URL entity in the workflow, then paste the target site and right click on the URL and then we will find many options that we can run to gather information, we will go with the all transforms and check each and every section manually to see what information each transform gives.
5. First, we have to checks for the different DNS for that we have to select the transform (To DNSNames [within Properties]

Below image shows the output of that transform:

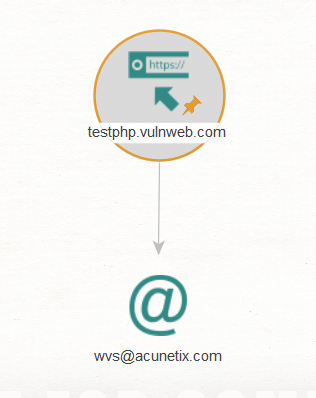
1. Now we will check for the domains and use the transform (To Domains [within Properties].

Below image show the output of the transform:



1. Now checking for e-mail if there any available on the website, for that we will use the transform “To E-Mail Addresses [within Properties]”.

Below image is the output of the email we found on website:



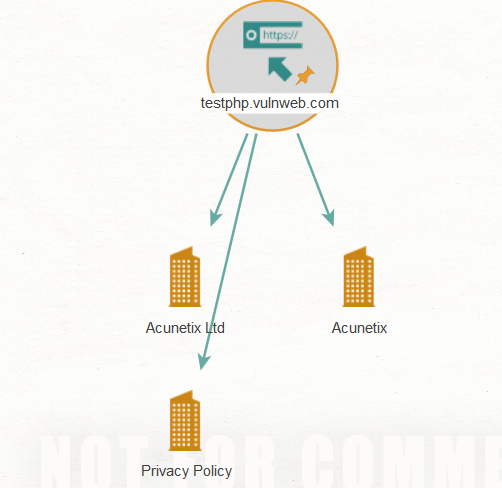
1. Now checking if we get any phone number from the website, for that we will use the transform “To Phone number [found on this we page]”.

Below image shows the result of phone number as requested by us:



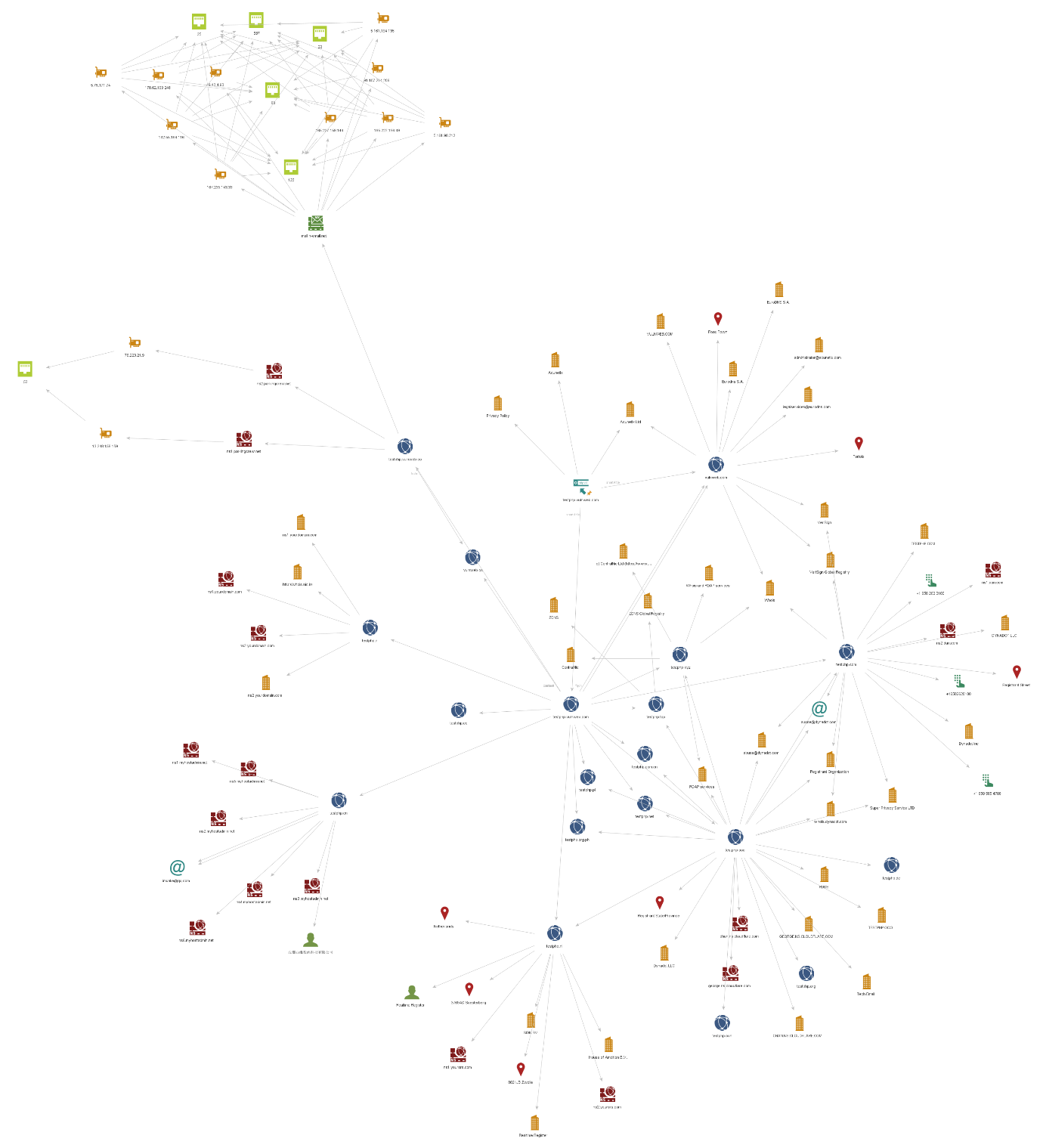
1. Now we will search for the different entities on the website, for that we will use the transform “To Entities [IBM Waston]”

Below shows the result:



After studying deeply in gathering information i got to know about many other different sub-parts of the results. And the below graph shows the detailed information about the target website.

Here’s the result:



**CONCLUSION**

In conclusion, after gathering huge amount of sensitive data, I came to know that how our sensitive data which are very important in aspects of the security for the company are easily available on the internet that can be used by the scammer and the hackers to exploit and damage the company with their bad intensions. In this we got to know about phone numbers, Gmail accounts, location, many IP addresses and their ports, few persons connected to the company, and many other things related to the company. Maltego GUI provides many tools to check these vulnerabilities if there available in our web pages. This helps to make our web pages more safe and secure and we can conduct these vulnerabilities assessments and penetration testing time to time as required.