## Lab 10-01: Information Gathering Using Dmitry

### Scenario

A cybersecurity analyst conducting surveillance for a client's network security assessment utilizes Dmitry, a powerful information-gathering tool. With Dmitry, the analyst efficiently gathers comprehensive information about the client's domain, including subdomains, IP addresses, email addresses, and open ports. The analyst identifies potential vulnerabilities and entry points that malicious actors could exploit by analyzing the data collected. Armed with this valuable intelligence, the analyst provides actionable insights to the client, enabling them to strengthen their cyber defenses and mitigate risks effectively.

### Solution

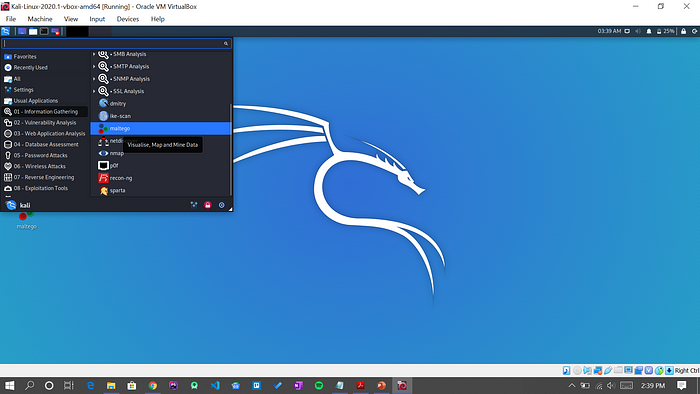
To enhance information gathering using Dmitry, the cybersecurity analyst ensures proper configuration and utilization of the tool's features. They customize Dmitry's parameters to target specific domains and maximize the scope of information collected. Additionally, the analyst employs advanced techniques such as DNS enumeration and port scanning to uncover hidden assets and potential vulnerabilities. By leveraging Dmitry effectively, the analyst generates valuable insights that empower informed decision-making and proactive risk mitigation efforts for the client's network security.

|  |
| --- |
| 1. Open your terminal. Open your terminal and move to the Desktop directory.    2. Create a new directory called Dmitry by using the command **mkdir Dmitry.**    3. Now, clone the Dmitry file. Clone the Dmitry file by using **git clone** [**https://github.com/jaygreig86/dmitry.git**](https://github.com/jaygreig86/dmitry.git). It will clone all the necessary files from the server. Make sure you are in the Dmitry directory.    4. Now, you need to check the clone file.  You can see a new directory here called dmitry using the command **ls**. Move to this directory using the following command and list the content using the following commands. **cd dmitry** and then usethe command **ls.**    5. Now, you need to install some directory.  You need to install the directory of **automake autoconf** using the command **sudo apt install makeauto autoconf.**    7. All the dependencies have been downloaded; now, you have to permit the tool using the following command. **Chmod +x configure.**    8. Now, permission has been given.  Permission has been given to the tool for execution. It is time to initialize the configuration file using the following command. **./configure.**    9. This is the time to make a configuration available for the tool. Use the command **make.**    10. Install the tool. Now, install the tool using the following command. **Make install./**    11. Now run the Dmitry.  These are some options that you can use.  **-o Allows the user to specify a location to write the output of the application.**  **-i This flag performs a whois lookup on the target's IP address.**  **-w This flag Performs a whois lookup on the host's domain name.**  **-n This flag Retrieves all available Netcraft information for a given target.**  **-s This flag is used to search all subdomains of the target.**  **-e This flag is used to search all emails associated with the target.**  **-p This flag performs TCP port scanning and finds open ports of the target.**    12. You can run the command like **dmitry *websitename.*** |

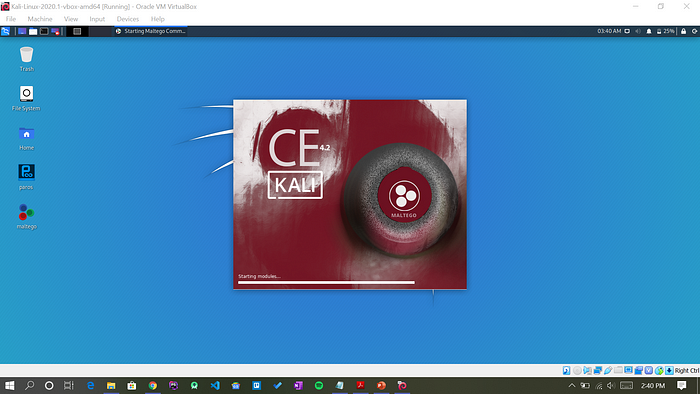
### Maltego

Maltego is a GUI-based open-source intelligence and forensics tool that reveals connections and relationships between information. It uncovers both direct and indirect links, providing a more detailed picture of the information landscape. The tool can provide a holistic view of individuals, including their social media profiles, mutual acquaintances, associated companies, and relevant websites. It can also map out the relationships between domain names, DNS records, and network blocks, offering a comprehensive view of an entity's digital footprint. Maltego is particularly useful for cybersecurity professionals and investigators looking to gather detailed intelligence on a target's infrastructure.

To open Maltego, navigate to **Information Gathering** **>** **Maltego**.



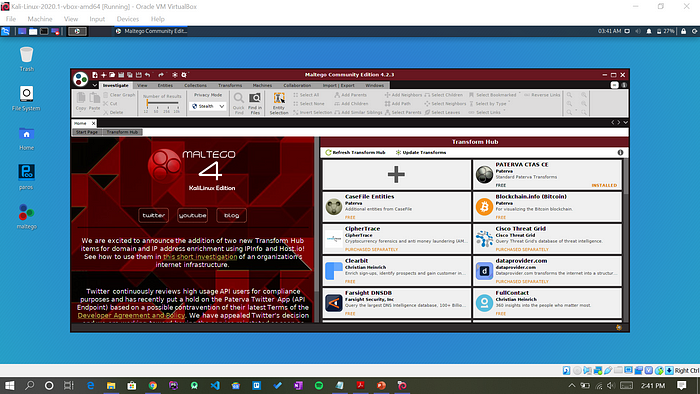
*Figure 10-12: Matltego Launch-1*



*Figure 10-13: Maltego Launch-2*

The homepage will look like the figure below.

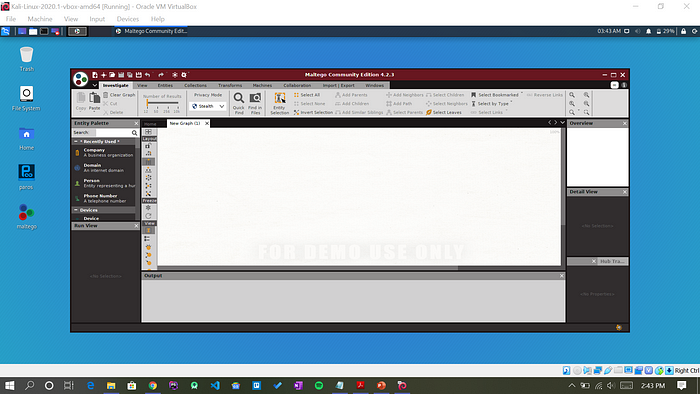
To create a new empty page, navigate to the top-left (3 dots in the circle) and select the **New** button.



*Figure 10-14: Maltego Homepage*

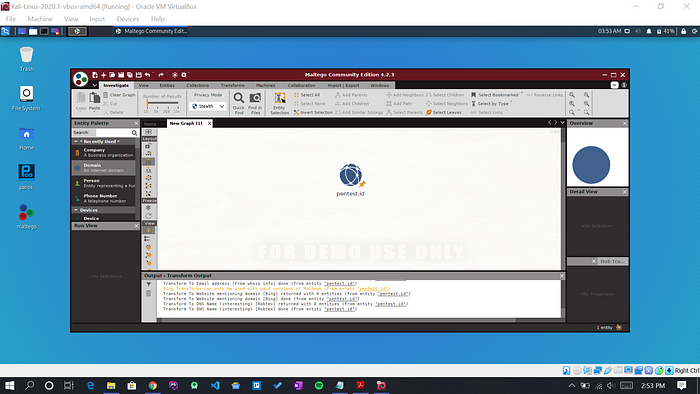
An empty white blank page appears.

On the left side, there is an Entity Palette that contains the Company, Domain, Person, Phone Number, etc.



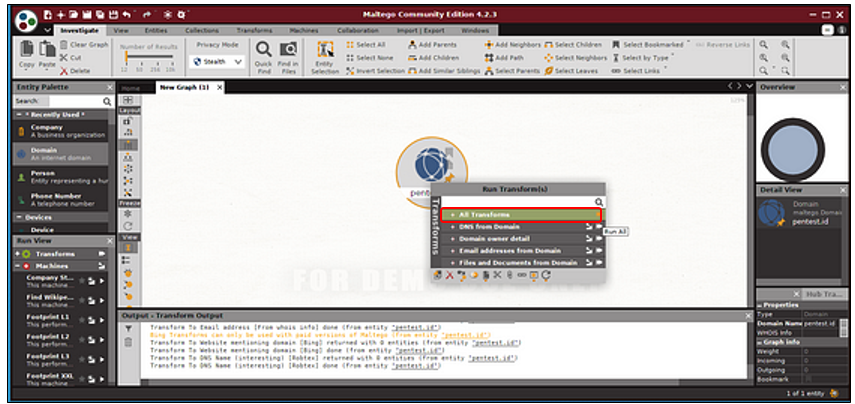
*Figure 10-15: Maltego Entity Palette*

Drag and drop the **Domain** entity onto the page, then enter the domain name.



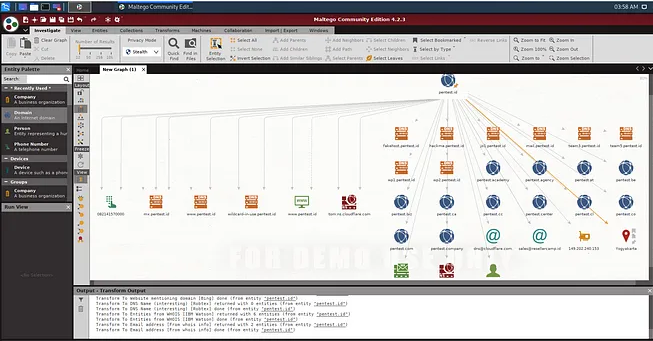
*Figure 10-16: Domain Entity*

To access all transform options, right-click and select the **All Transform** button.



*Figure 10-17: Domain Entity*

After completing the Transform process, you will see the result as shown in the figure 10-18. You can view specific domain details, such as email, person, and server.



*Figure 10-18: Maltego Output*

You can also acquire further information by using another entity, such as a company, person, or phone number.