Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals

Lab File – CA 02

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

To explore and learn Maltego (an open-source intelligence and forensics application) for gathering information about a target and represents in an easily understandable format.

Requirements :

- Virtualisation Software
- Kali Linux 2021.4a
- Basics of Maltego
- Administrator privilages
- Internet Connection

Objectives :

To Run different Transforms and find following information :

- ✓ Domain Name System & Entity related details
- ✓ People, phone numbers, email addresses related details
- ✓ Historical snapshots and Important files related details
- ✓ IP Adresses and Website Technologies and Relationships

Procedure :

Basics

Currently, there are three versions of the client, and we will be using Maltego Community Edition 4.2.19 for this practical.

1> Open root terminal in kali linux, and run the command `sudo apt install maltego` to install maltego.
2> Launch the application by searching `maltego` from Applications button in taskbar.
3> From the title bar, click New icon or Ctrl + T.

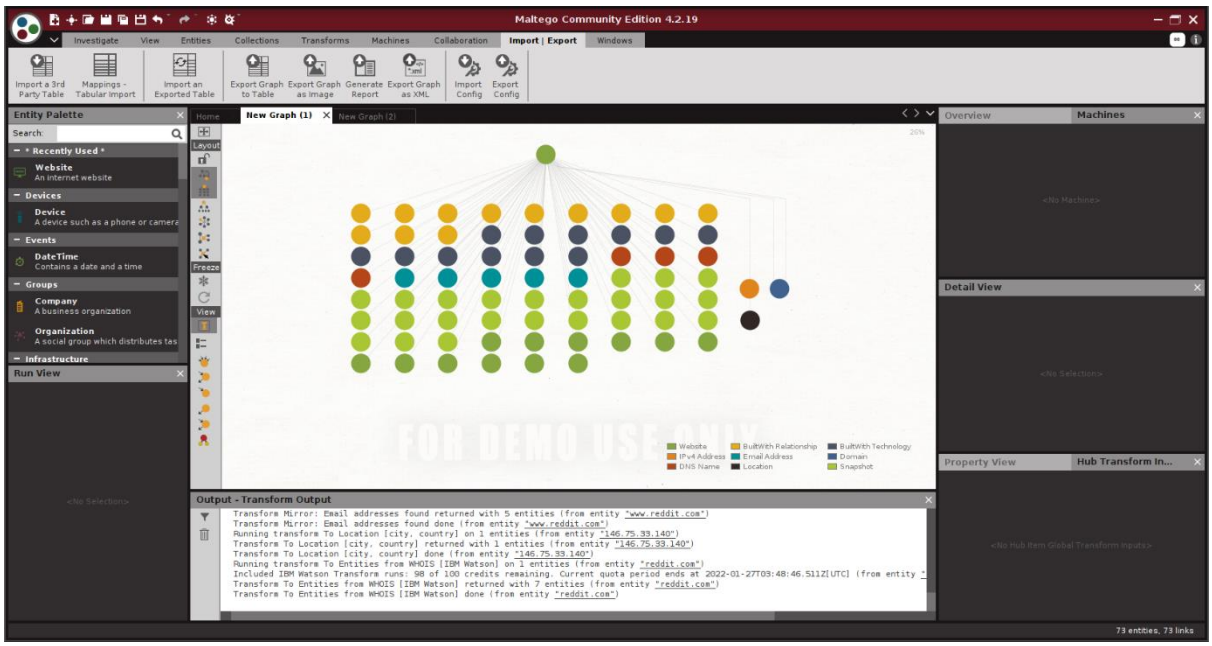
The extreme left 'Entity Panel' provides with the list of types of entities present in the software, whereas below lies the 'Infrastructure tab' which basically contains all transforms or scripts that could be run in the entities to obtain information.
In the Tabs section, we also have 'Import/ Export', helpful to generate reports and tables for the obtained information.

Website Information

1> Search ‘Website’ from Entity panel and drag-and-drop it on the blank graph. Double click and rename it the the target site, say www.reddit.com.

2> Right-click and select Double Arrow of ‘All Transforms’ from the drop down Run Transforms, to obtain detalis like: Domain, Entity Properties, IP Addresses Web tech & Relationships etc. A dialog box appears.

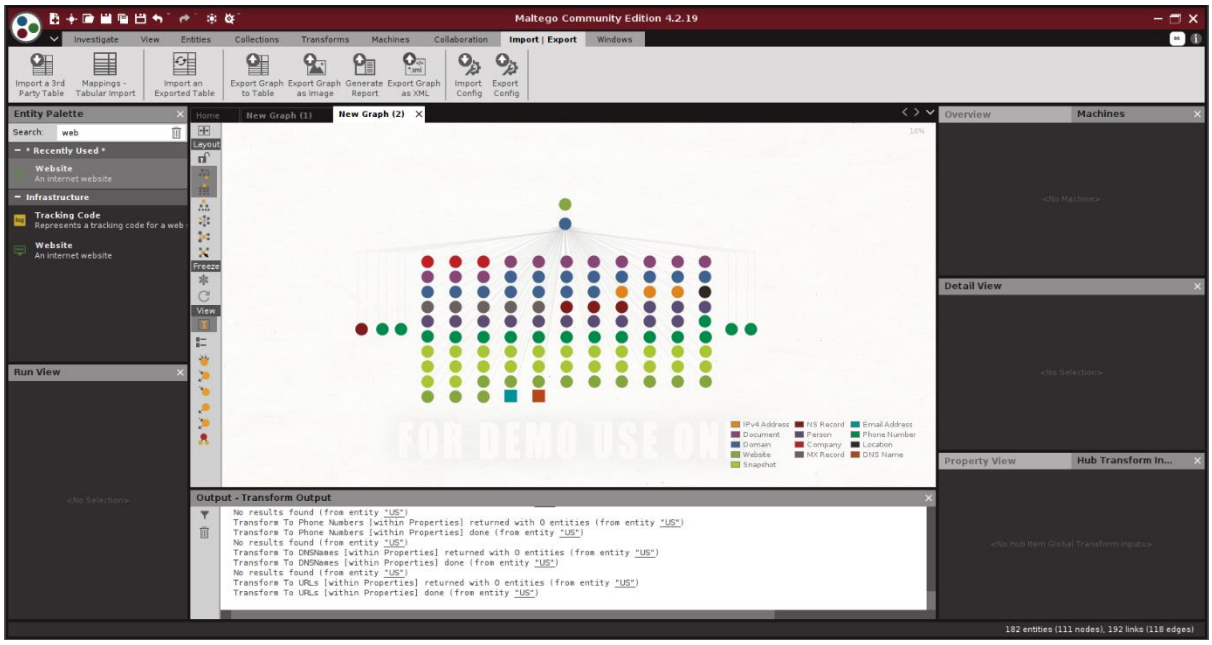
3> Set the duartion range in the wayabck machine section, to obtain links of older versions of the site. In dns name section, increase padding to 20 to obtain clear results. Click ‘Run’. Information obtained are as follows:



As we ca see, in this zoomed out version, all types of information obtained are classified according to its types in the index.

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/drive/folders/19upnHnKXo7k3vXxKCR5QyL6FecHu3UJD?usp=sharing

1> Following similar step, as did while obtaining information from website, we end up with the website entity being shown in a blank graph.
2> Right-click and select Double Arrow of 'Convert to Domain' from the drop down Run Transforms, and we get the Domain Entity stating redddit.com.
3> Again, Right-click and select Double Arrow of 'All Transforms' from the drop down Run Transforms, to obtain detalis like: Domain, People, Emails, Phone Numbers, Documents, Locations, MX & NS Records, Company, IP Addresses etc.
4> Set the duartion range in the wayabck machine section, to obtain links of older versions of the site. Click 'Run!'.
Information obtained are as follows:



As we ca see, in this zoomed out version, all types of information obtained are classified according to its types in the index.

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/drive/folders/1PvKTzPNR2Tdourk8g27YUt9pwrmYPSUn?usp=sharing

To Generate Reports

After reguired information in obtained at the graph, head over to 'Import/ Export' from the Tabs Section. Different options for exporting graphs are present there, like:

Export graph to Table

1> Selecting `Export Graph to Table` option provides us with a wizard.
2> In Setting Step, select whole graph from export section, check remove duplicates, select human/ machine readable as wish and check separate link file. Click Next.
3> In Select File Step, change to the desired location where we want our graph to be saved, putting desired file name and selecting desired file type. Click Next.
4> It now, displays the changelog. Click Finish.

Export graph as Image

1> Selecting `Export Graph as Image` option provides us with a dialog box.
2> Change the desired saving loaction of the file, provide filename, change the file type as wish, set image zoom to any value above 100 and image bounds to whole graph.
Click Save.

Generate Report

1> Selecting `Generate Report` option provides us with a dialog box.
2> Change the desired saving loaction of the file, provide filename, change the file type as wish, set graph image bounds to whole graph and check all include options. Click Save.

Conclusion :

Maltego is a powerful tool, you can extract a broad type of information through the network, technologies, and personnel (email, phone number, twitter).
By extracting all this information, an attacker can perform different type of malicious activity.
The built-in technologies of the server: attackers might search for vulnerabilities related to any of them and simulate exploitation techniques.
SOA information: also, can be useful for attackers, they can abuse this information to find vulnerabilities in their services and architectures and exploit them.
Name Server: attackers can exploit NS using malicious techniques like DNS hijacking and URL redirection.
IP addresses: attackers can abuse the IP address by scanning and searching for open ports and vulnerabilities, and thereby attempt to intrude in the network and exploit them.
Geographical location: attackers can perform social engineering attacks to leverage sensitive information.