Name: Dhruva Kapadia
MIS: 111903142

Assignment 4

PENETRATION TESTING USING KALI LINUX

- **Maltego**

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiableWith Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape.Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 80 data partners, a variety of public sources (OSINT) as well as your own data.The different editions of the Maltego Desktop Client, data integrations, deployment and infrastructure options, support services and learning and training formats enable you to tailor Maltego to your specific needs in terms of capabilities, data access, and other requirements.

Associate an Email ID to a person

Step1: Fire up Kali and Start Maltego

Step2: Login in to your Maltego account

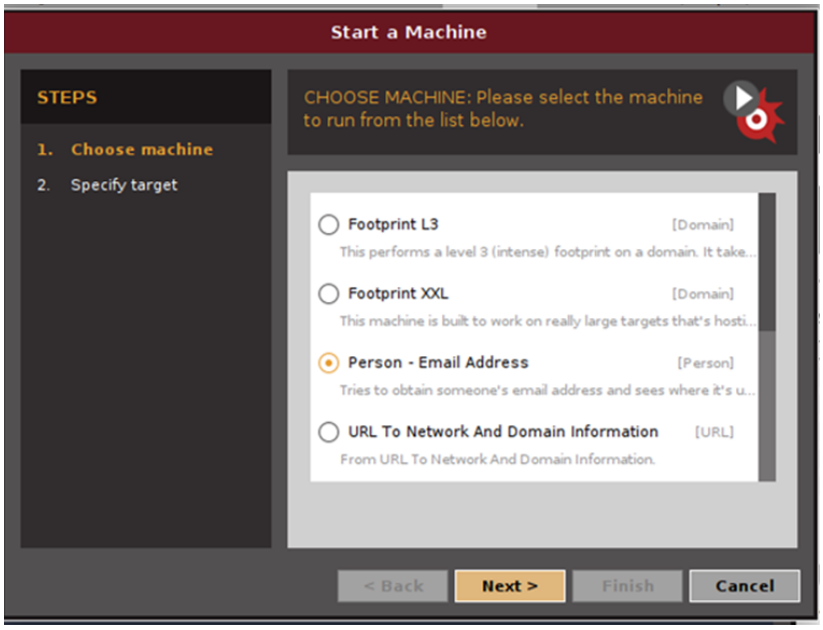
Step 3: Start a Machine

Step 4: Choose a target

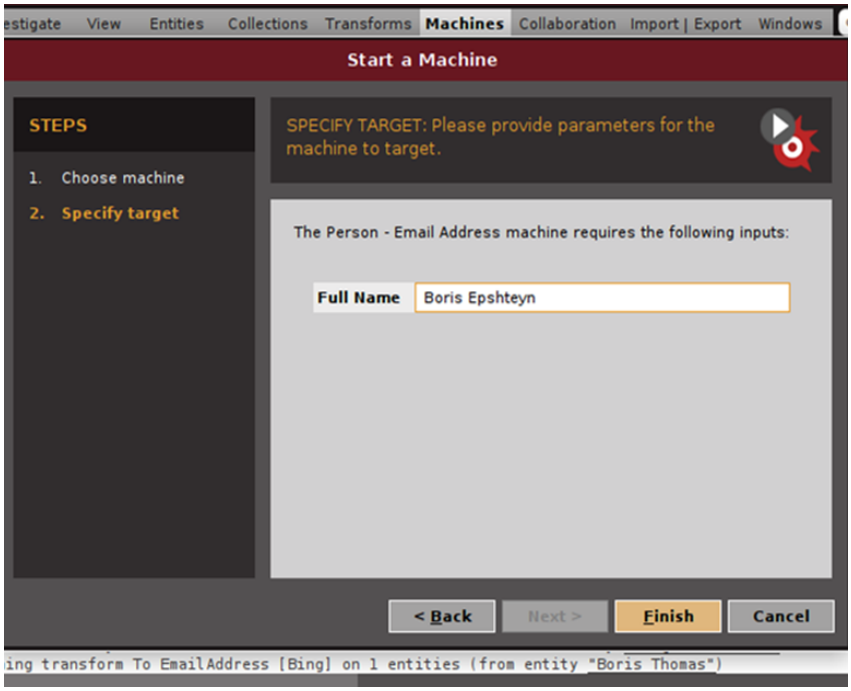
Step 5:Select the Appropriate Email Address

Step 6: Create a Graph of the Target

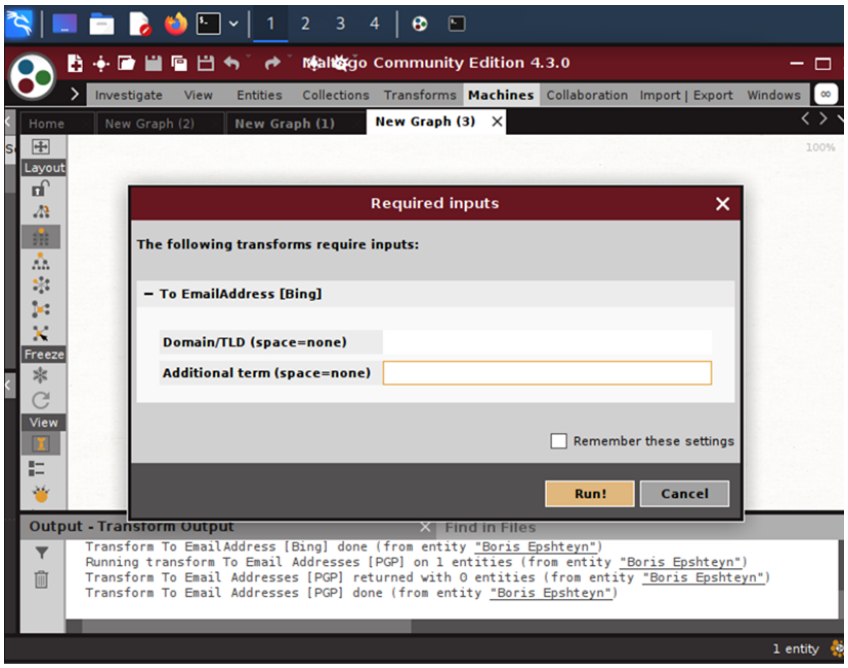
1. Associate an email to a person.

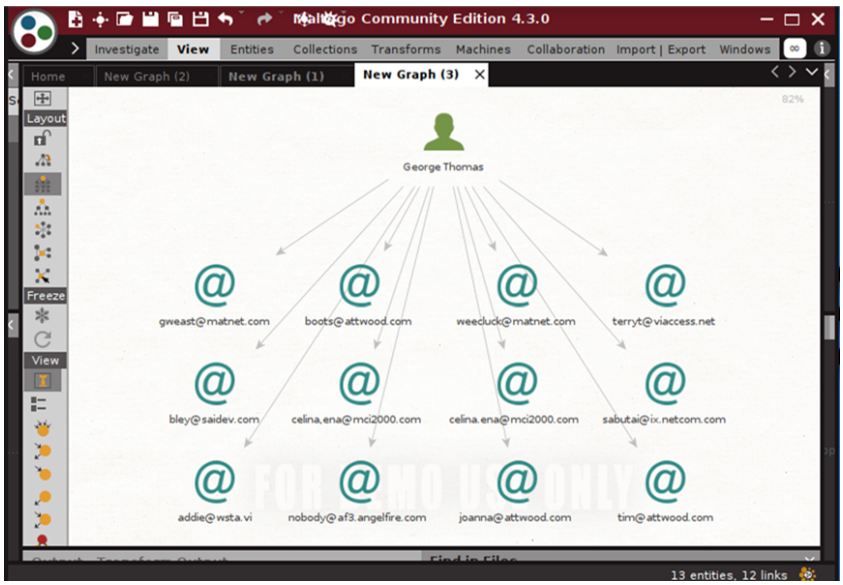


2. After you've set up your account, start the machine and select the type of reconnaissance you want to conduct on the target to link an email address to a person.(as per above diagram).

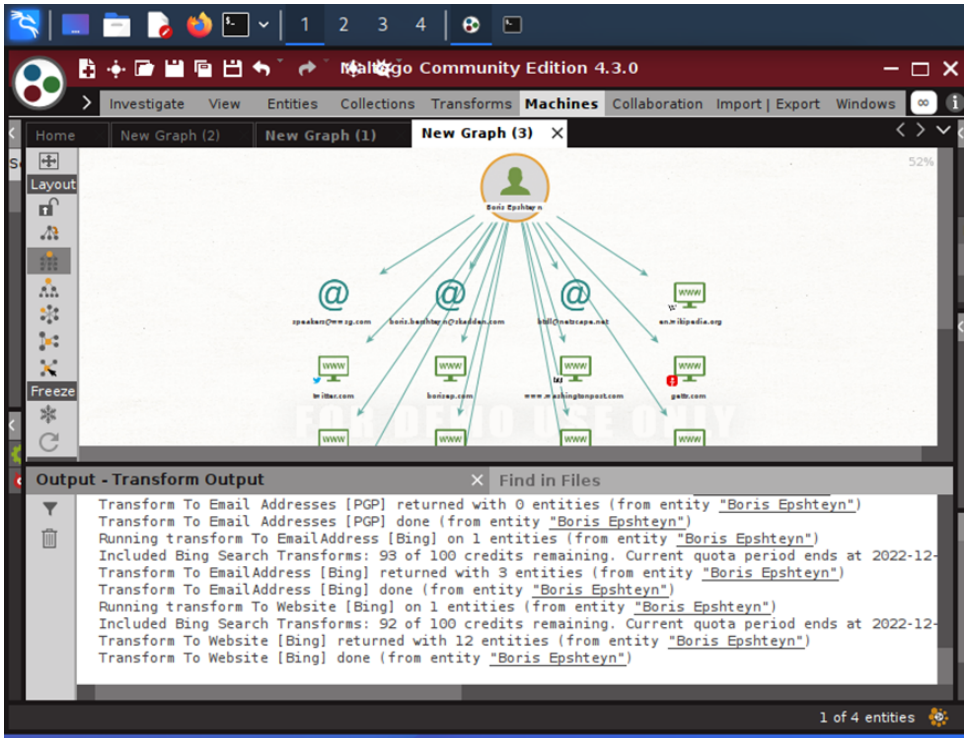


3. Maltego delivers a transform Output in the form of a graph that illustrates the entities returned when you enter the person's name and press Finish.





4. Associate website to a person
   Using the transform on the name node on the graph, we get websites associated with the person. The websites will get appended on the graph. However, in this example no websites are returned. Hence the graph remains as it is. Transform To Website [Bing] returned with 0 entities.



- **Vega**

Vega helps you find and fix cross-site scripting. SQL injection and more. Vega is free and open source security scanner.
First Download vega zip file from https://subgraph.com/vega/download.html site.
Unzip and run vega in the terminal.
Scan www.nullbyte.com

- **Nmap : To scan local network**

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Step1: Open command line.

Step2: Install nmap.

Step3:Get the ip of your network.

Step 4: Scan network for connected device(s) with nmap

```
└─$ nmap 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-09 15:18 IST
Nmap scan report for 10.0.2.15
Host is up (0.000090s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

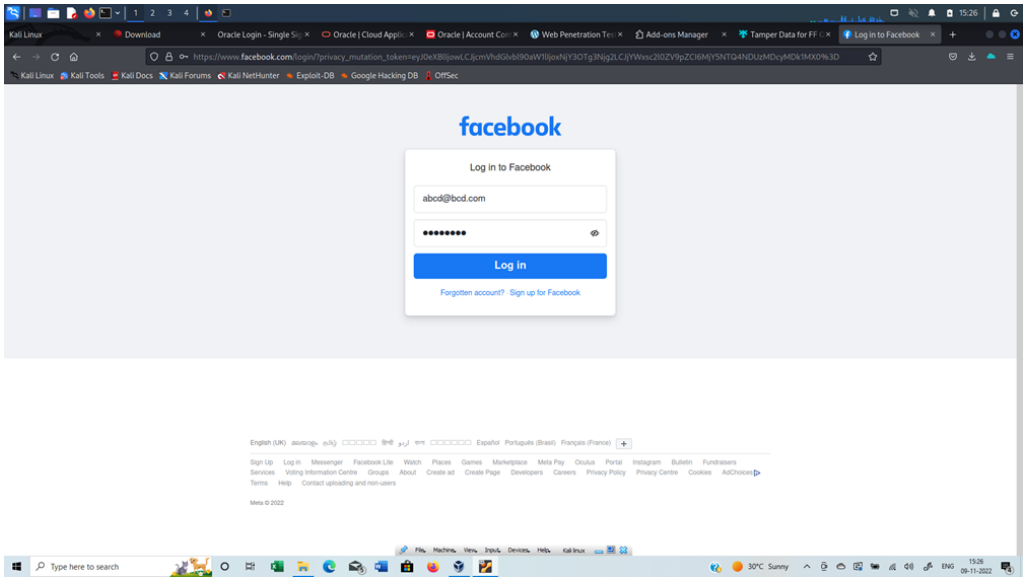
- **<u>Tamper Data Plugin</u>**

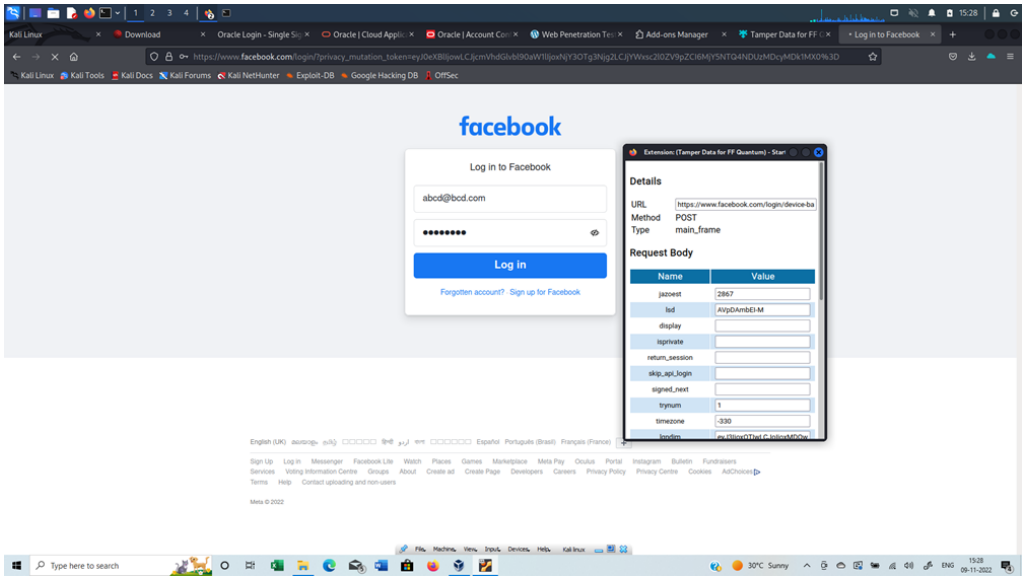
Tampering is the way of modifying the request parameters before request submission. Tampering can be achieved by various methods and one of the ways is through Tamper Data. Tamper data is one of the highly used extensions in Firefox. It allows tampering of the data that is sent between the client and the server as well as easy access to GET and POSTING element's data. Using this plugin, we are able to modify the headers and parameters for POST and GET requests that are sent, using this we could possibly fake our identity and do malicious activities. - Monitor live requests - Edit headers on live requests - Cancel live requests.

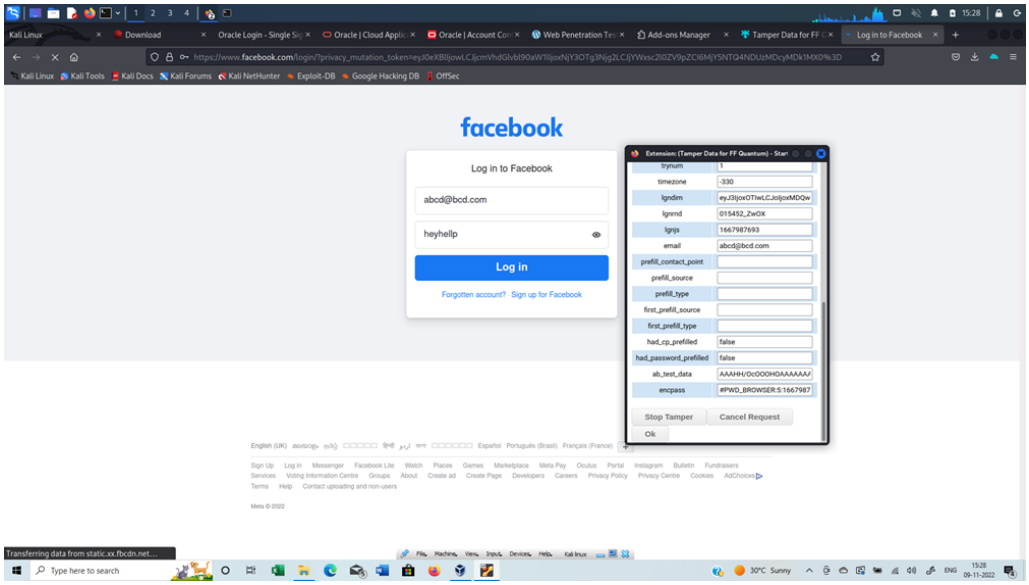
Step 1 : Install the Tamper Data Add-On

Step 2 : Open any website , eg Facebook and enter email and password, but start the Tamper data add on before pressing login.

Step3 : The data in the POST request will be seen in the plugin

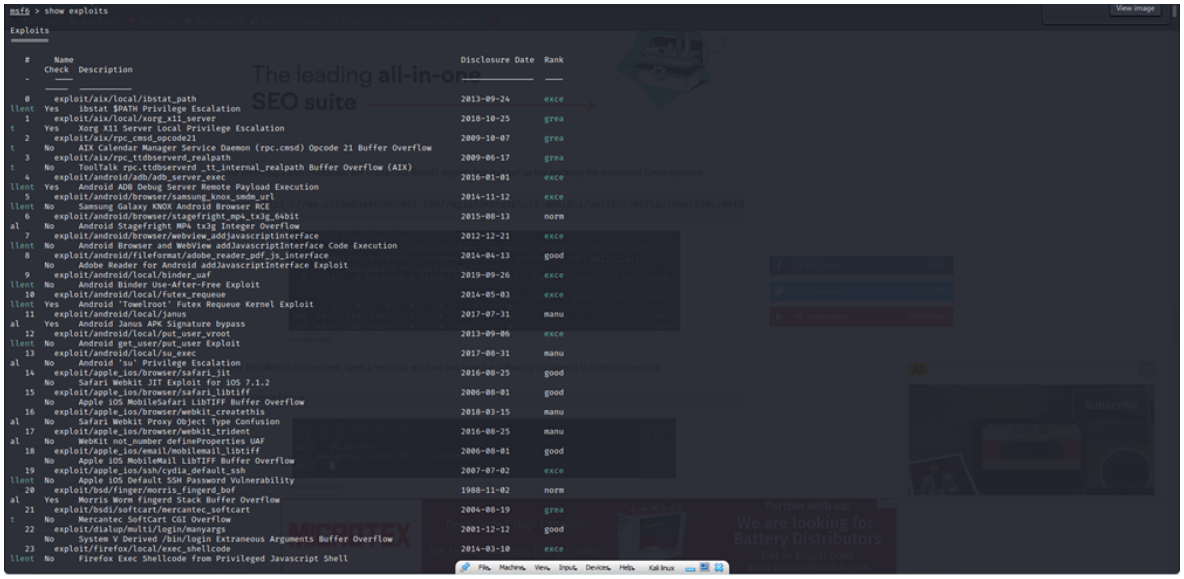






- **<u>Metasploit Exploits</u>**

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.



These are the available Exploits in Kali Linux.