Name - Manish Arora Mis - 111803036 BTech Comp Div1 B1

PENETRATION TESTING IN KALI LINUX

What is Penetration Testing ?

Penetration testing, also called Pentest, is a cybersecurity process that helps you stay ahead of hackers. In a pentest, an ethical hacker finds security vulnerabilities in your application, network, or system, and helps you fix them before attackers get wind of these issues and exploit them. This makes Pentesting a non-negotiable fundamental step for a website or business owner.

Penetration testing has become a necessity for a variety of sectors as the cyber threat landscape continues to deteriorate. This post will teach you everything you need to know about penetration testing for websites, networks, and applications.

1. **Maltego :**

   Maltego is an open source intelligence and forensics application. It will offer you time-consuming mining and gathering of information as well as the representation of this information in an easy to understand format.

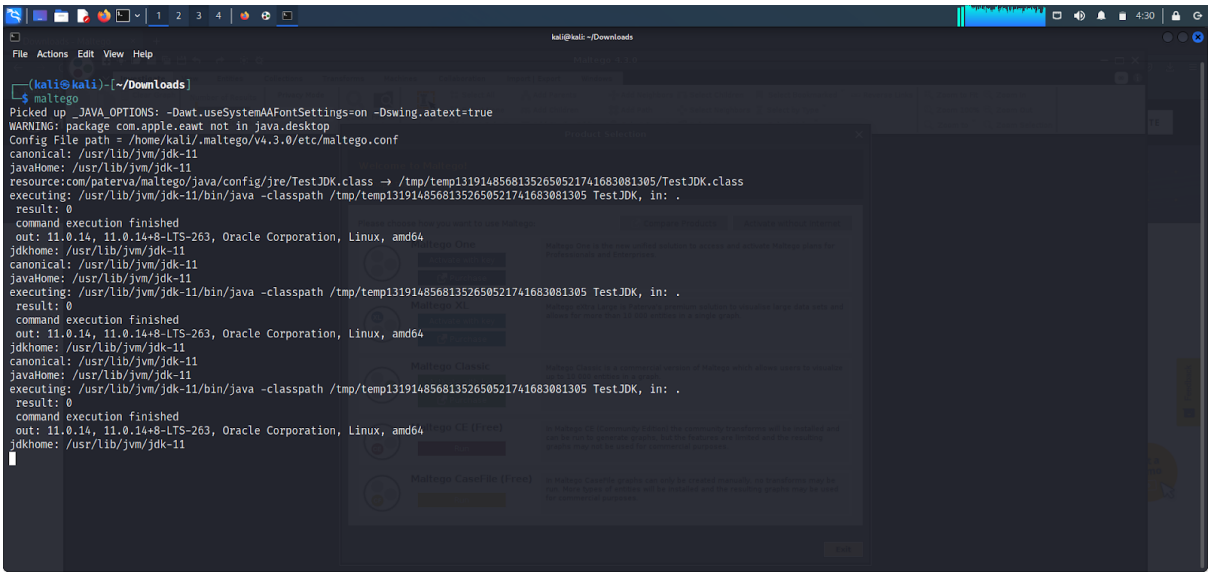
   This package replaces previous packages matlegoce and casefile.

   Maltego is open-source intelligence and forensics software created by Paterva in Pretoria, South Africa. Maltego focuses on offering a library of transforms for finding data from open sources and presenting it in a graph format that may be used for link analysis and data mining. Maltego Technologies, based in Munich, Germany, has assumed responsibility for all global customer-facing activities as of 2019.

   Maltego supports the creation of custom entities, allowing it to represent any sort of data in addition to the software's standard entity types. The application's major focus is on evaluating real-world relationships between people, groups, Webpages, domains, networks, internet infrastructure, and social media affiliations (Social Networks, OSINT APIs, Self-hosted Private Data, and Computer Networks Nodes).

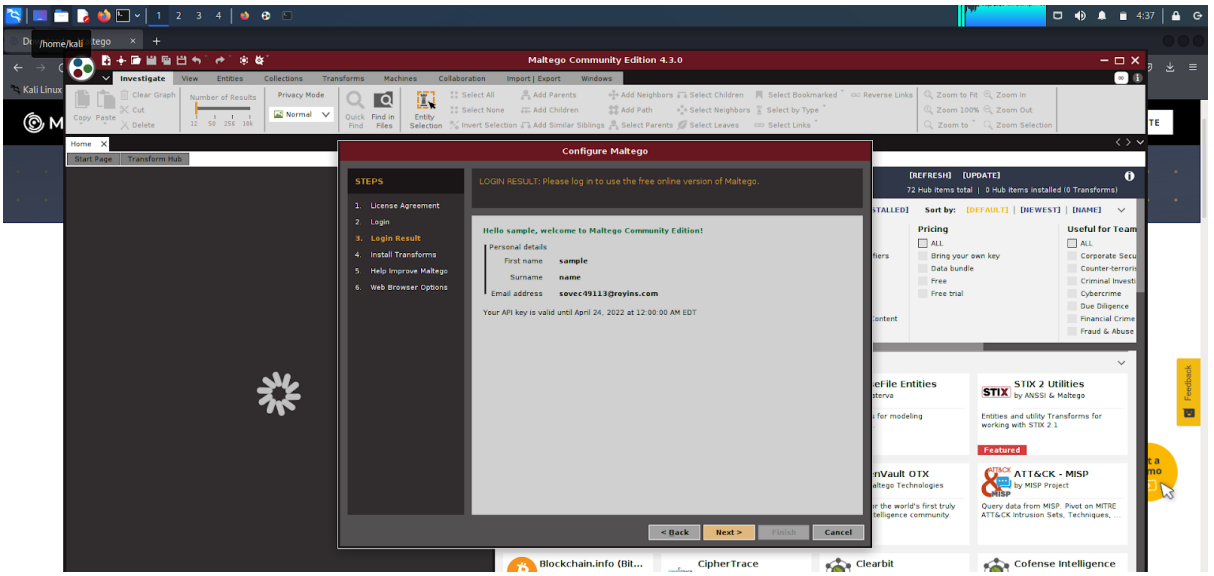
   Maltego extends its data reach with integrations from various data partners. Among its data sources are DNS records, whois records, search engines, social networking services, various APIs and various meta data.

To start maltego simply type “maltego” in the command prompt:

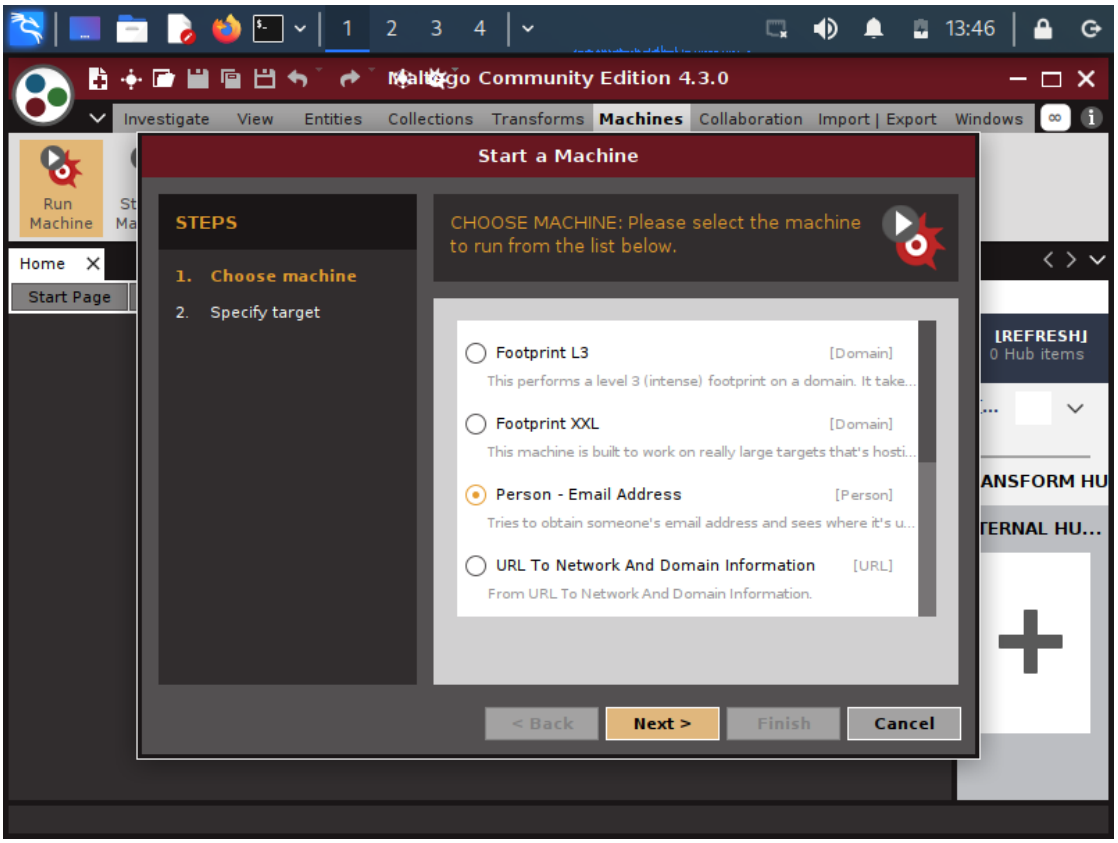


Register to Maltego by creating your account and login using the same credentials:
To login to the maltego, first We need to register on the website and fill in the requested details, then we can login to our maltego account.

Login process will be completed and a welcome screen will be shown there. It’s an indication that we have logged into our account.

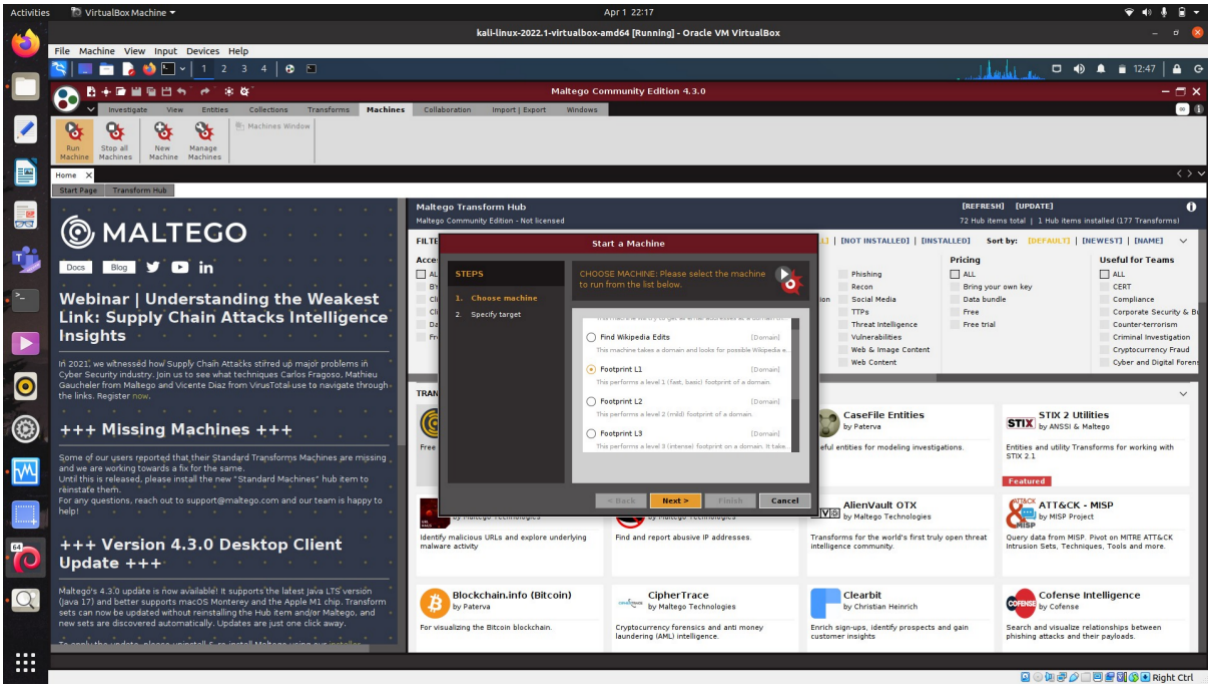


After you've set up your account, start the machine and select the type of reconnaissance you want to conduct on the target to link an email address to a person.
Refer to the following image for the same…



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. We may then use additional transforms on each of these devices to create a more detailed map of the target.

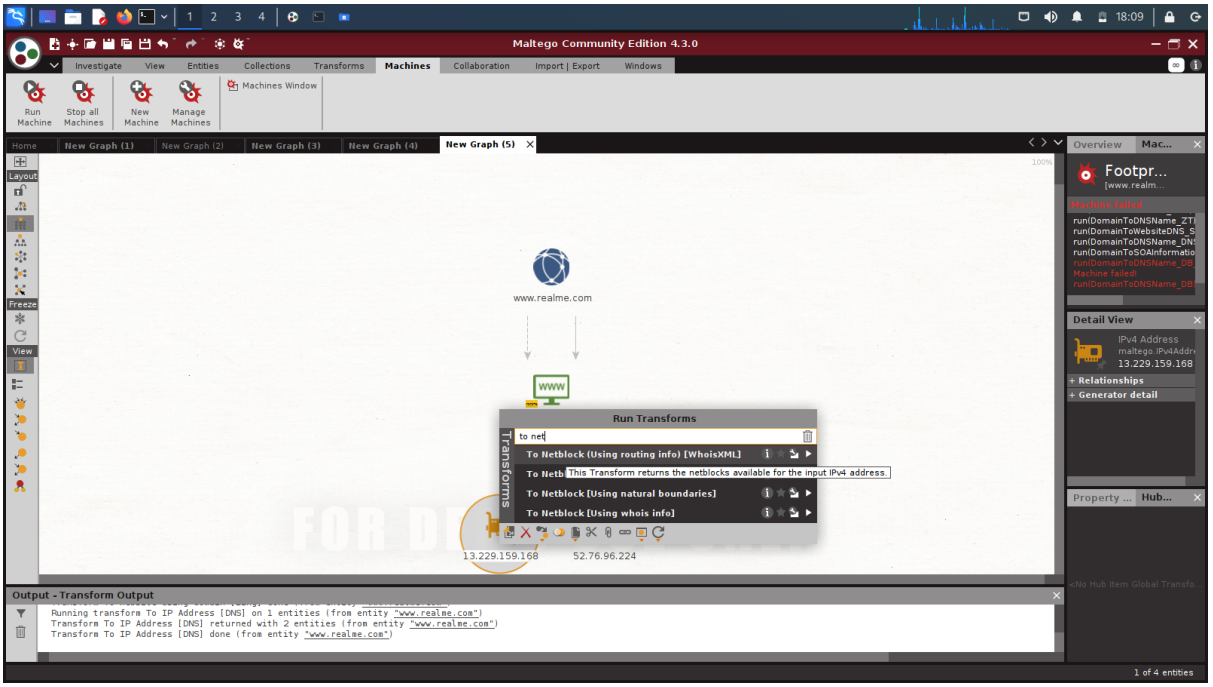
To link a website to a person, start a machine and select Footprint 1 from the type of reconnaissance menu. This is a basic footprint of a domain in its most basic form.

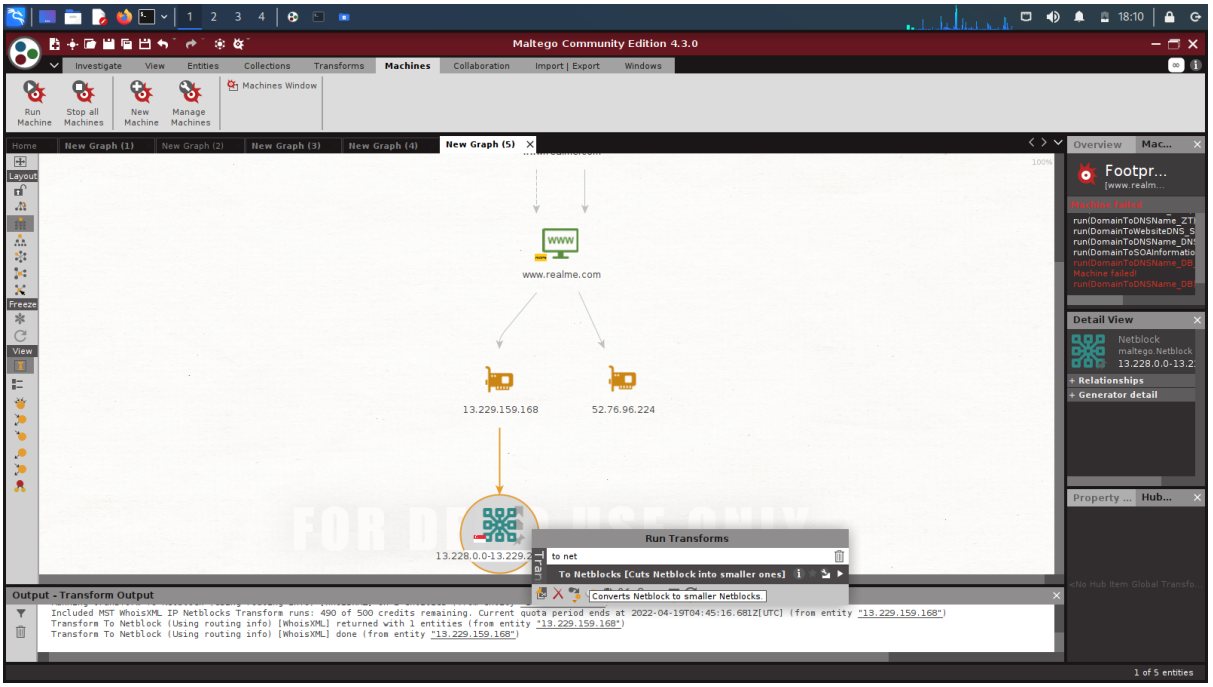


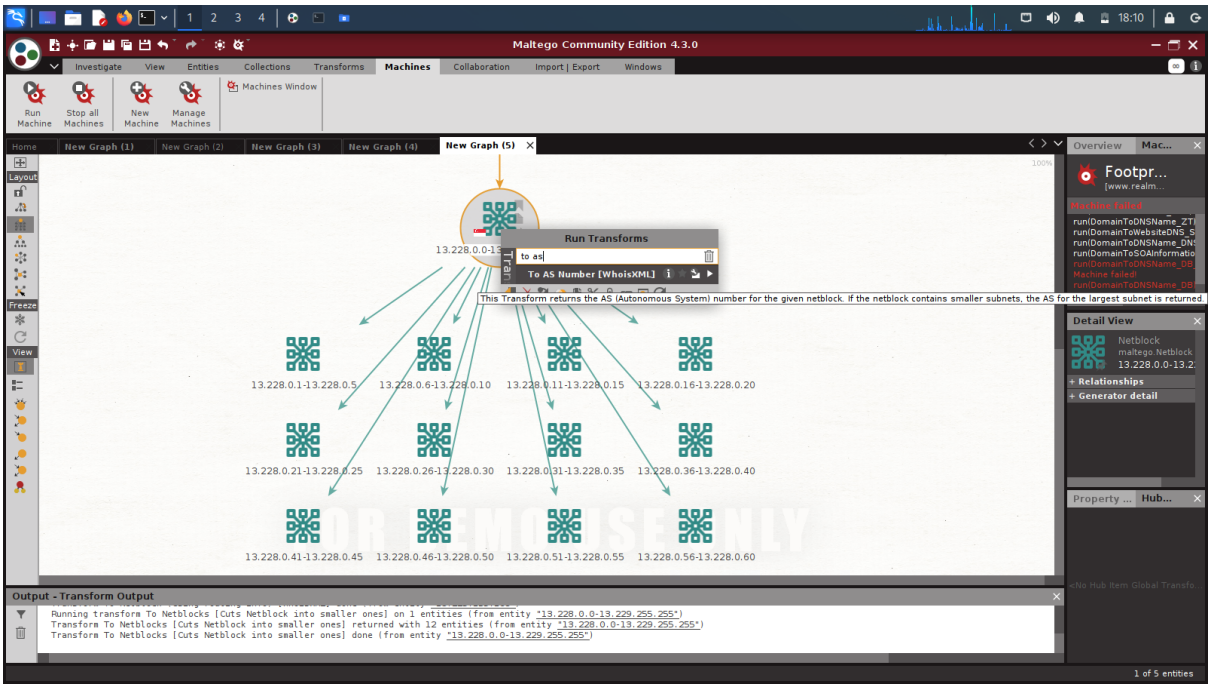
Let's us take a look of footprint on the website : www.realme.com

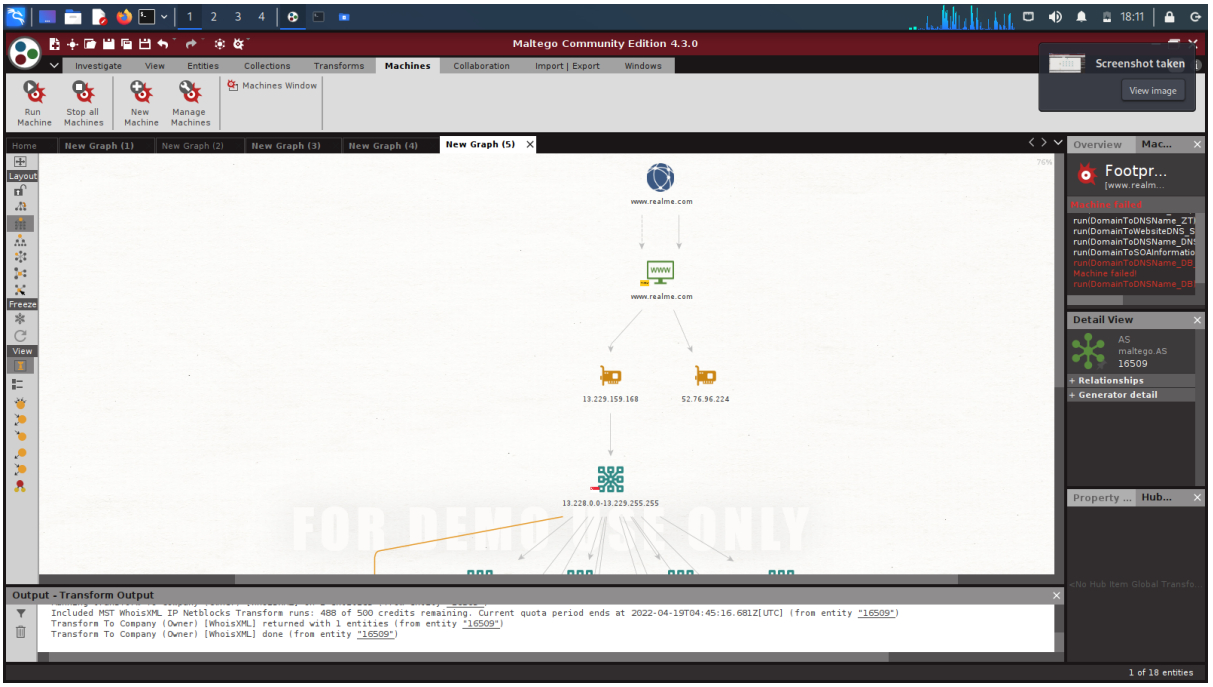
Add the website in the domain name to get the insights of the specified website.

After you click Finish, Maltego will begin Footprinting the domain for you. The Footprint transform is shown in motion in the Transform output, and we can see what it's looking for. Aside from the domain you filled in, the graph displays other information such as the IP address, Netblock, and so on.



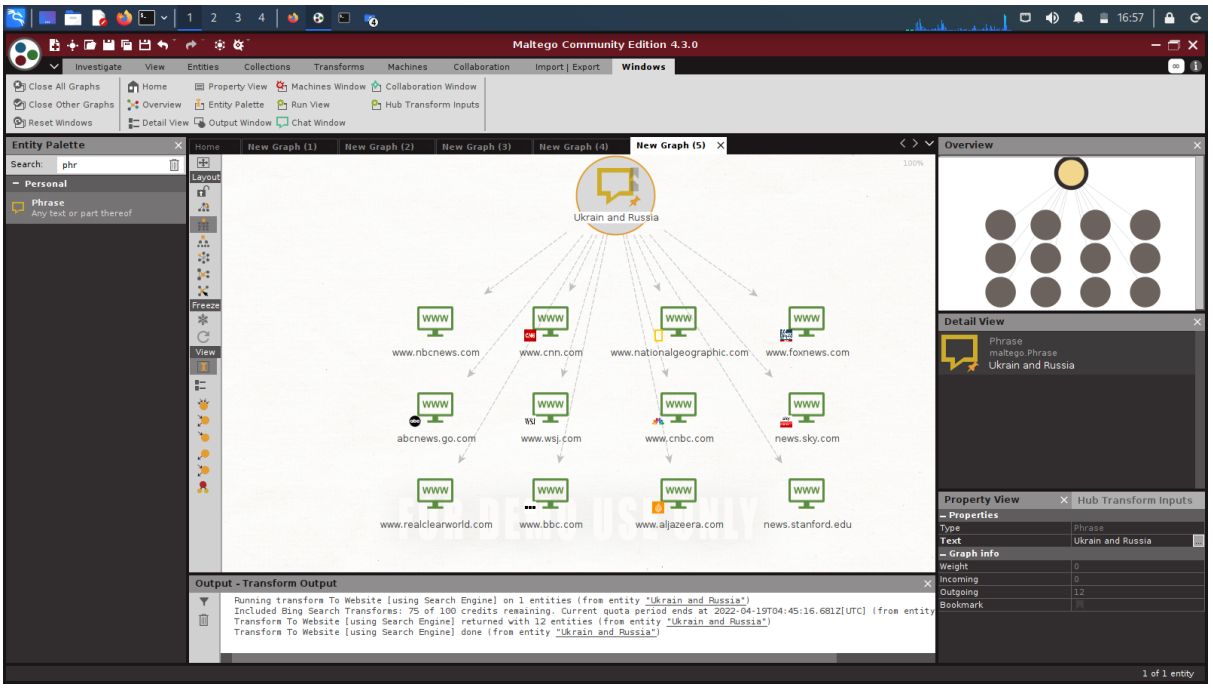

Maltego Community Edition 4.3.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Run Machine
Stop all Machines
New Machine
Manage Machines
Machines Window
New Graph (1)
New Graph (2)
New Graph (3)
New Graph (4)
New Graph (5)
www.realme.com
13.229.159.168
52.76.96.224
13.228.0.0-13.229.2
Run Transforms
to net
To Netblocks [Cuts Netblock into smaller ones]
Converts Netblock to smaller Netblocks
Output - Transform Output
Included MST WhoisXML IP Netblocks Transform runs: 490 of 500 credits remaining. Current quota period ends at 2022-04-19T04:45:16.681Z[UTC] (from entity "13.229.159.168")
Transform To Netblock (Using routing info) [WhoisXML] returned with 1 entities (from entity "13.229.159.168")
Transform To Netblock (Using routing info) [WhoisXML] done (from entity "13.229.159.168")
Overview
Detail View
Property ...
1 of 5 entities

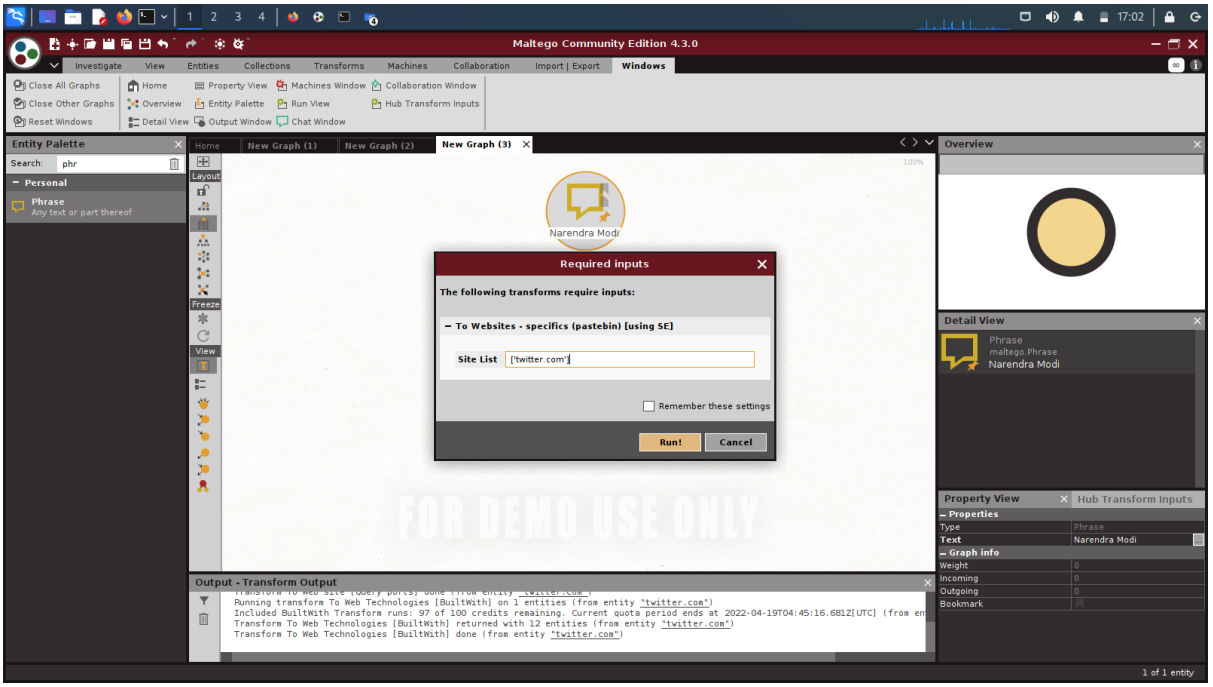

Maltego Community Edition 4.3.0
Run Transforms
to as
To AS Number [WhoisXML]
This Transform returns the AS (Autonomous System) number for the given netblock. If the netblock contains smaller subnets, the AS for the largest subnet is returned.
13.228.0.1-13.228.0.5
13.228.0.6-13.228.0.10
13.228.0.11-13.228.0.15
13.228.0.16-13.228.0.20
13.228.0.21-13.228.0.25
13.228.0.26-13.228.0.30
13.228.0.31-13.228.0.35
13.228.0.36-13.228.0.40
13.228.0.41-13.228.0.45
13.228.0.46-13.228.0.50
13.228.0.51-13.228.0.55
13.228.0.56-13.228.0.60
Output - Transform Output
Running transform To Netblocks [Cuts Netblock into smaller ones] on 1 entities (from entity "13.228.0.0-13.229.255.255")
Transform To Netblocks [Cuts Netblock into smaller ones] returned with 12 entities (from entity "13.228.0.0-13.229.255.255")
Transform To Netblocks [Cuts Netblock into smaller ones] done (from entity "13.228.0.0-13.229.255.255")
1 of 5 entities

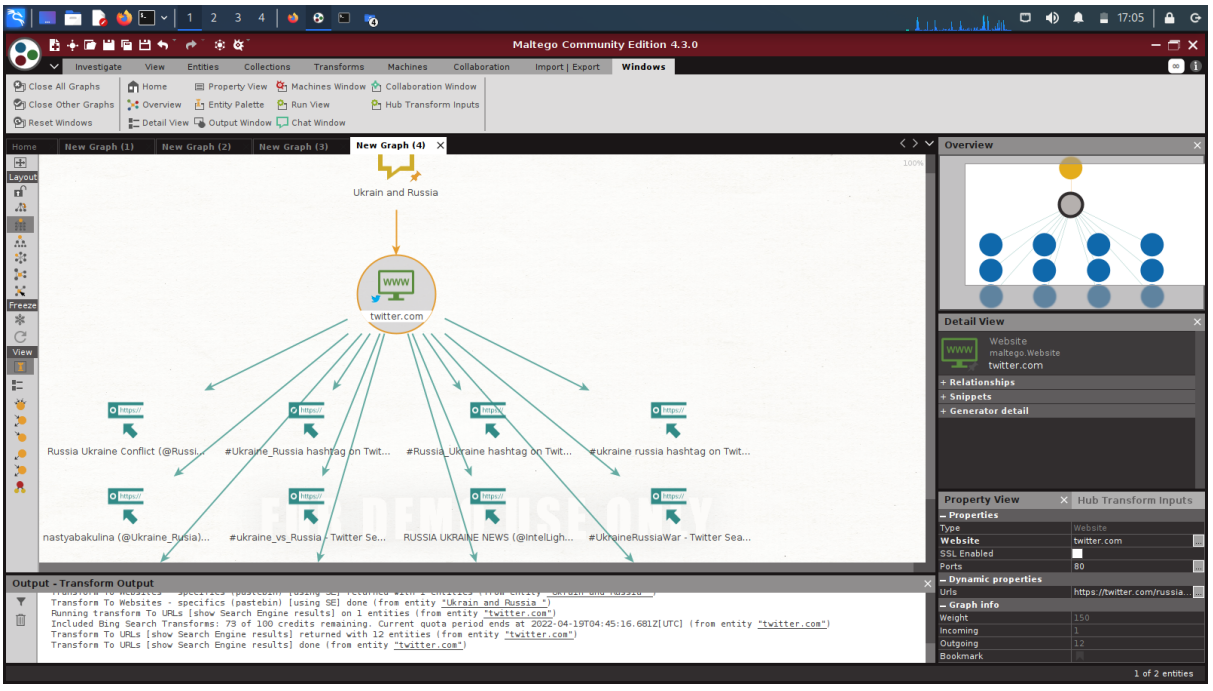


To verify an Email Address of a person drag and drop the email icon and right click on it to select the verify email transform. The output shows whether the email exists or not and returns an entity after verifying the address.

In order to extract geolocation from a tweet, we can use To Tweet Geolocation:- Just type any phrase and this transform will extract geolocations from that tweet.





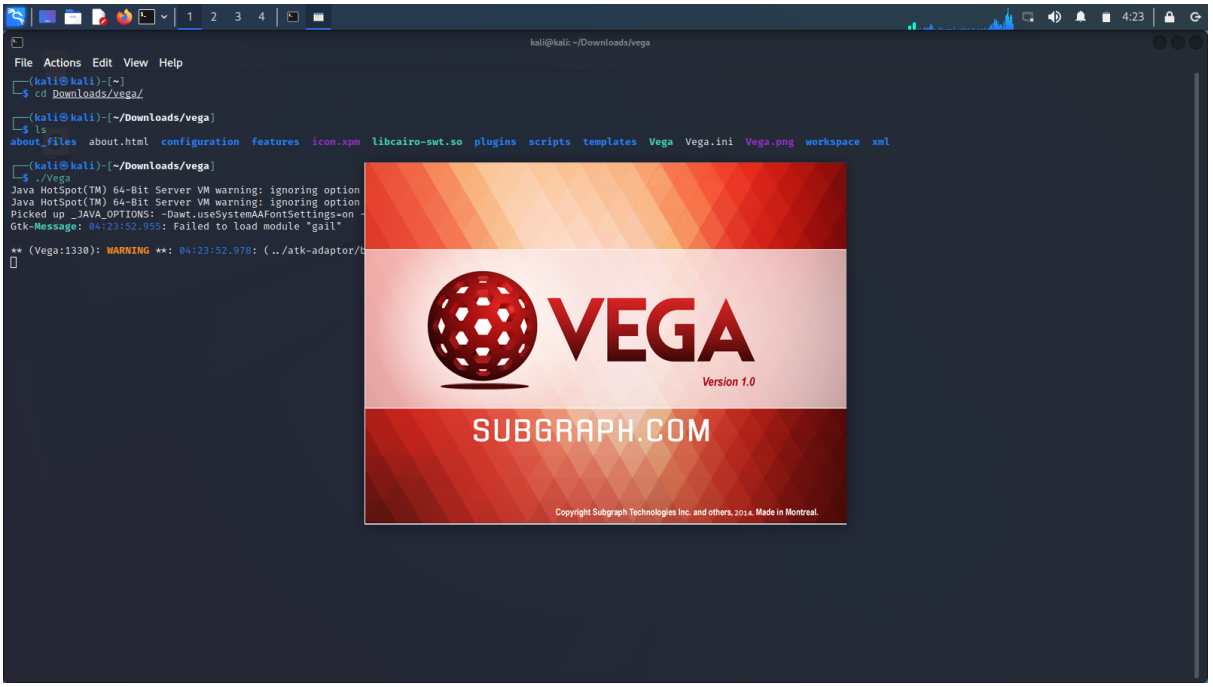


2. Vega

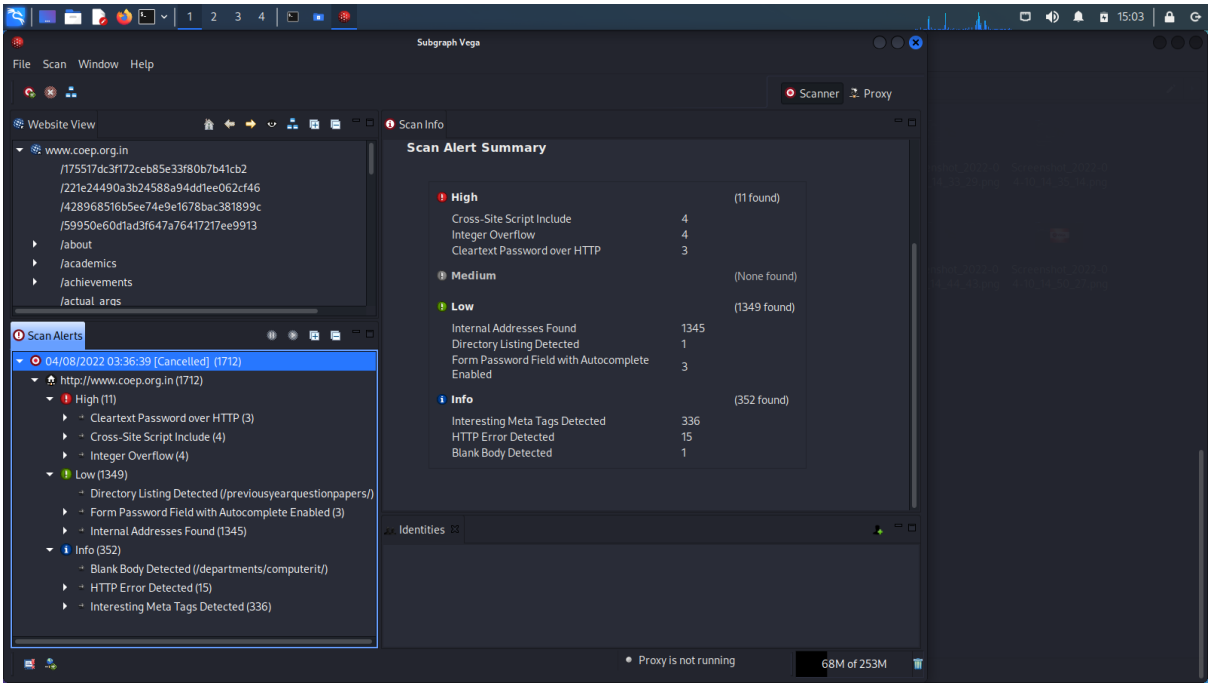
Vega is a free and open source web security scanner and web security testing platform to test the security of web applications. Vega can help you find and

validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java, GUI based, and runs on Linux, OS X, and Windows.

Vega can be started by typing the command ‘vega’:



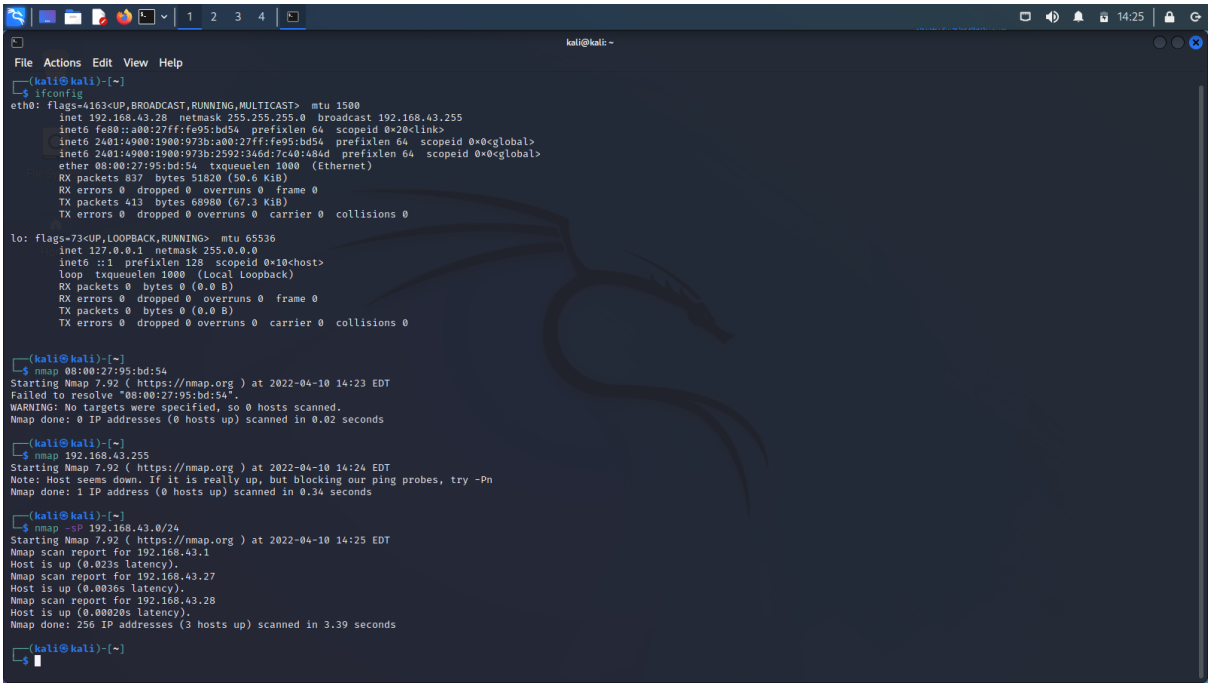
I submitted the COEP college webpage, which vega scanned. Cross-site scripting and Clear Text passwords had high security vulnerability flags.



3. NMAP

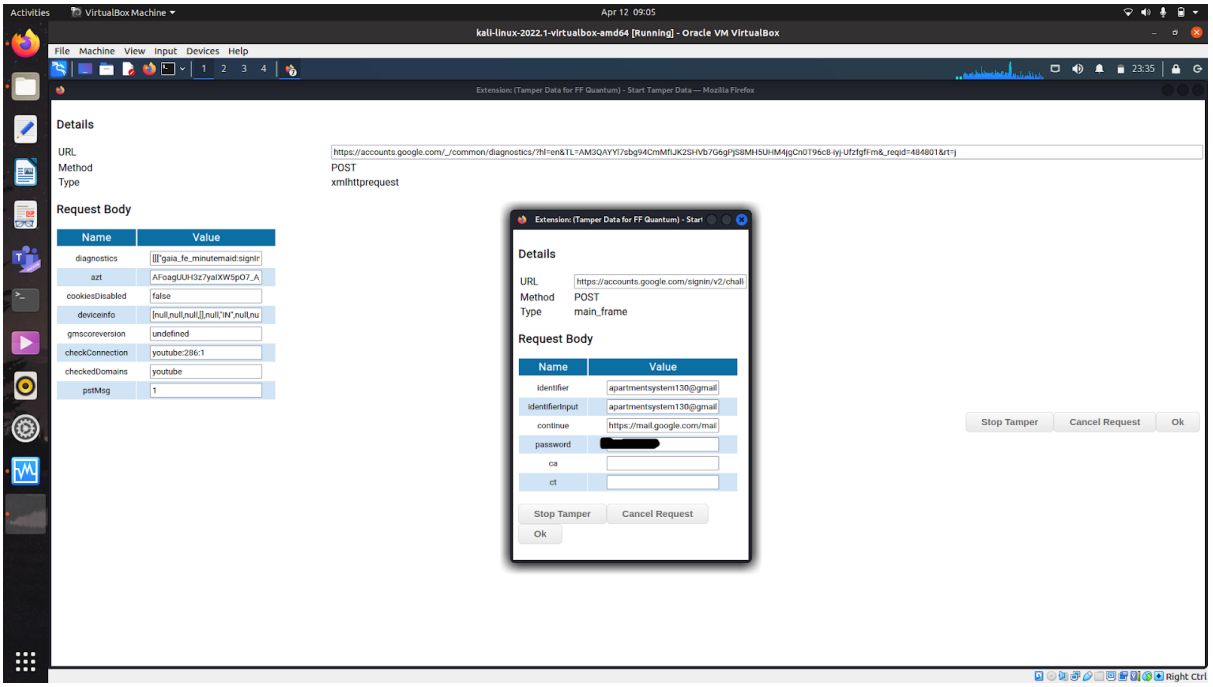
(Scrutinize your local network and submit a screenshot of the results.)

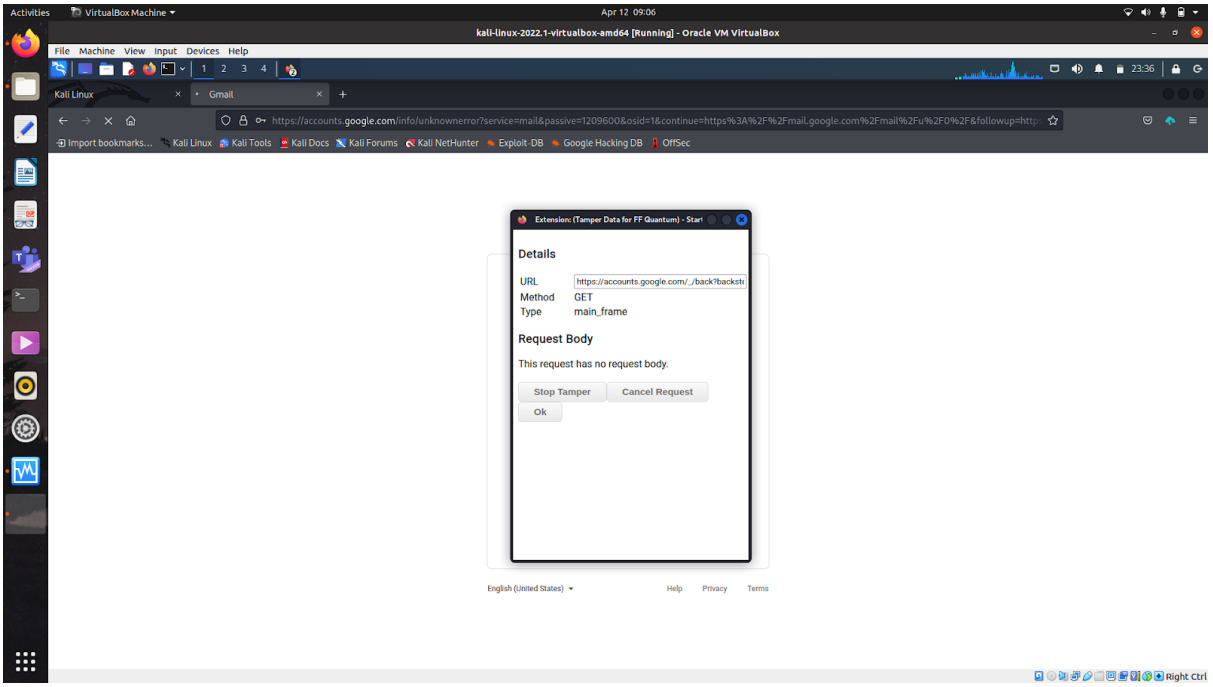
Install nmap on your system and use the command "ifconfig" to get your network's ip address. Look for connected devices on your local network.



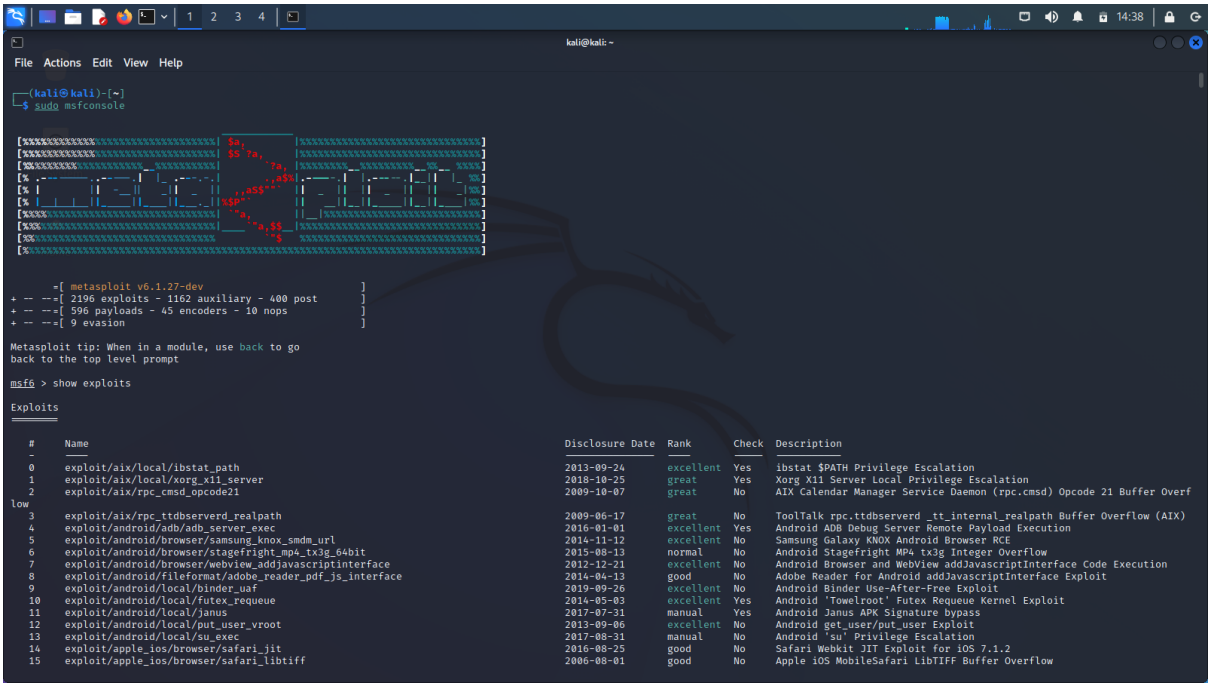
4. Tamper Data plugin in FireFox

Tampered Data is a Firefox add-on that allows you to inspect and change HTTP requests before they are sent. It displays information such as cookies and hidden form fields that your web browser sends on your behalf. We can alter the headers and parameters for POST and GET requests submitted using this plugin, allowing us to impersonate someone else and carry out harmful operations. Install the Firefox add-on. After installing the plugin, log in to your Gmail account and start messing with data before typing your password. It will display the details for your Gmail account's GET and POST queries.



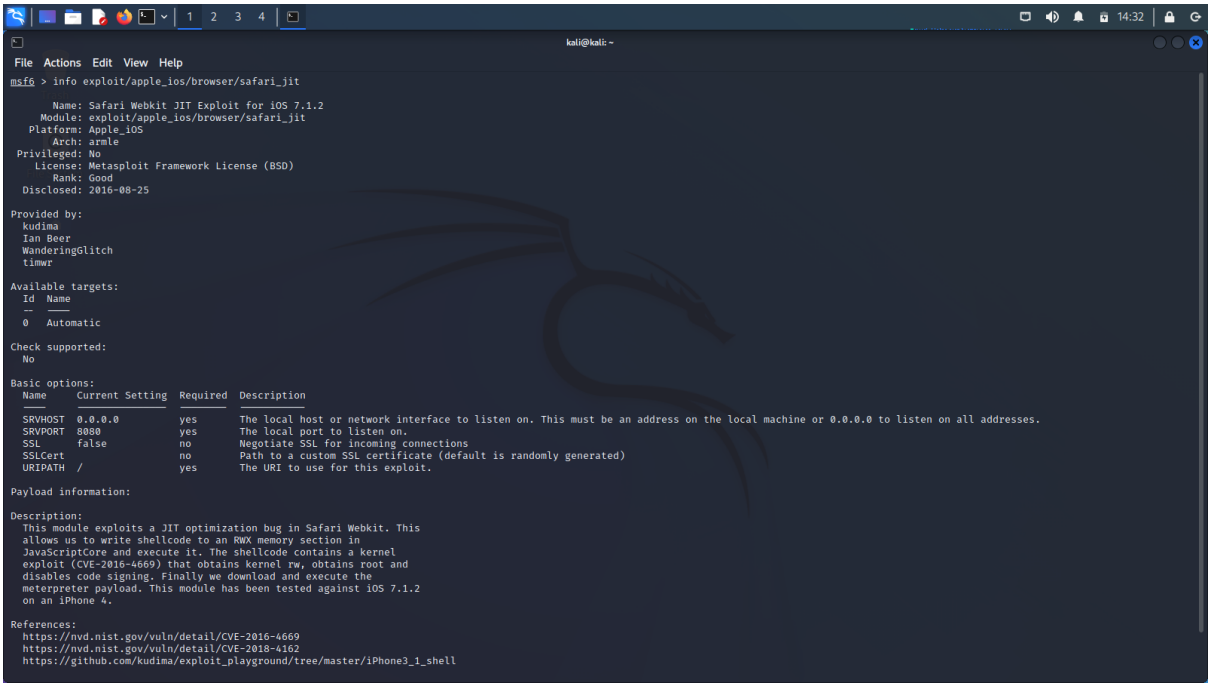


5. **Metasploit framework: List out all the exploits provided by Metasploit framework.**



op5 is a network monitoring application that is free and open source. In versions 7.1.9 and lower, the configuration page allows you to test a system command, which can be exploited to execute arbitrary code as an unprivileged user. The service will never be brought to a halt as a result of this exploit. SQL Injection, CMD execution, RFI, LFI, and other attacks fall into this category. Unless there are exceptional conditions, no conventional memory corruption attacks should be assigned this rating.

Name : op5 v7.1.9 Configuration Command Execution
Module : exploit/linux/http/op5_config_exec
Supported platform(s) : Linux, Unix
Target service / protocol : http, https
Target network port(s) : 80, 443, 3000, 8000, 8008, 8080, 8443, 8880, 8888



Name : Mutiny 5 Arbitrary File Upload

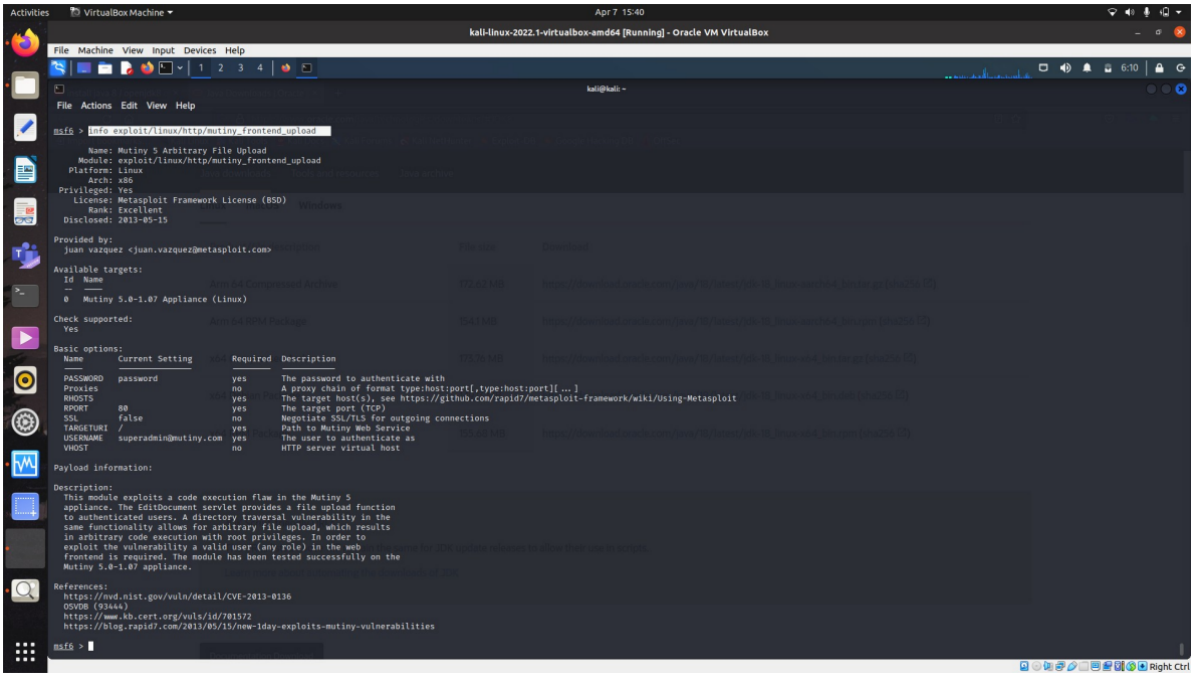
Module : exploit/linux/http/mutiny_frontend_upload

Supported architecture(s) : x86

Supported platform(s) : Linux

Target service / protocol : http, https

Target network port(s) : 80, 443, 3000, 8000, 8008, 8080, 8443, 8880, 8888



Name : MobileIron MDM Hessian-Based Java Deserialization RCE

Module : exploit/linux/http/mobileiron_mdm_hessian_rce
Supported architecture(s) : cmd, x86, x64
Supported platform(s) : Linux, Unix
Target service / protocol : http, https
Target network port(s) : 80, 443, 3000, 8000, 8008, 8080, 8443, 8880, 8888

This module takes advantage of an ACL bypass in MobileIron MDM solutions to run a Groovy gadget against a Java deserialization endpoint based on Hessian. The service will never be brought to a halt as a result of the exploit. This is true for SQL Injection, CMD execution, RFI, LFI, and other similar attacks. Unless there are exceptional circumstances, no conventional memory corruption exploits should be assigned this ranking.

Reliability :

- **Repeatable-session:**
  The module is expected to get a shell every time it runs.

Stability:

- **crash-safe:**
  Module should not crash the service.