

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 :

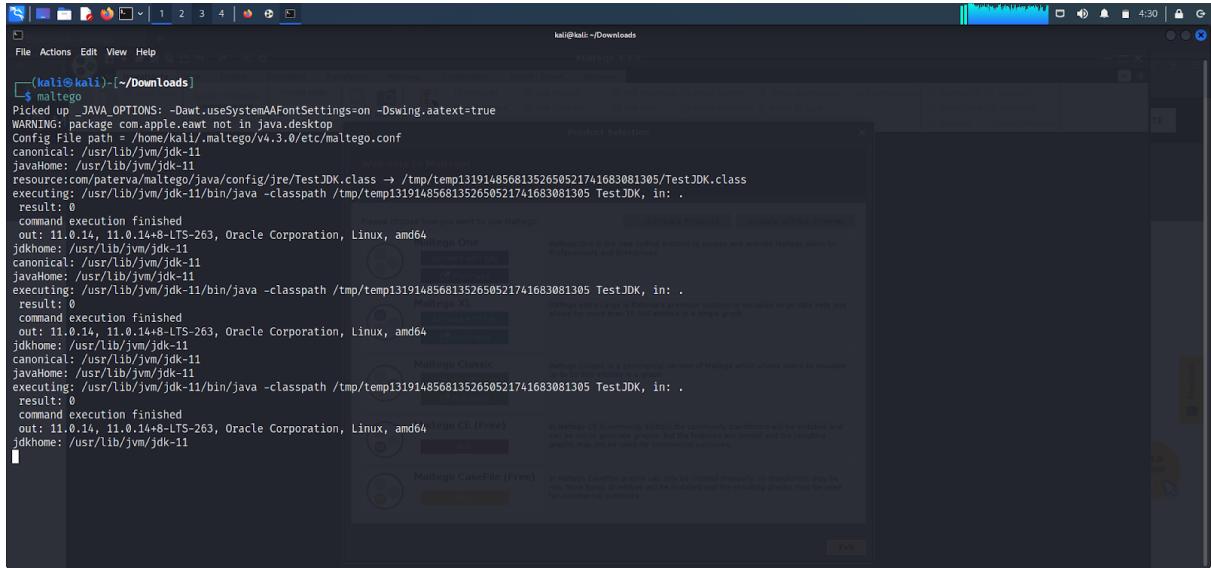
Maltego is an open source intelligence and forensics application. It will offer you time-consuming mining and gathering of information as well as the representation of this information in an easy to understand format.

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.

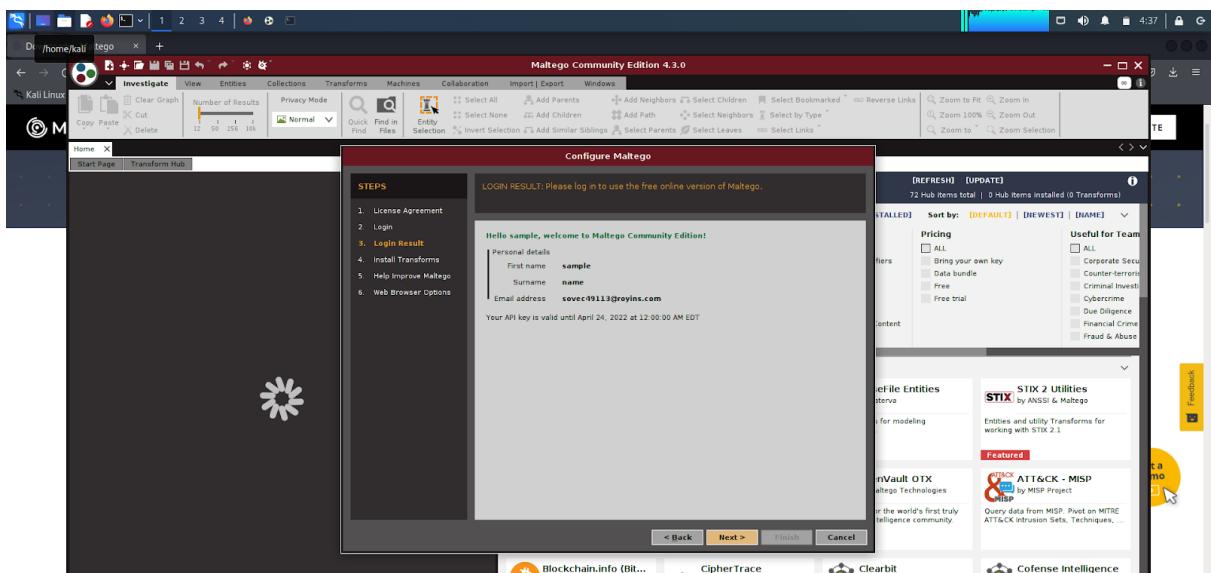
To start maltego simply type “maltego” in the command prompt:



```
(kali㉿kali)-[~/Downloads]
$ maltego
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
WARNING: package com.apple.eawt not in java.desktop
Config File path = /home/kali/.maltego/v4.3.0/etc/maltego.conf
canonical: /usr/lib/jvm/jdk-11
javaHome: /usr/lib/jvm/jdk-11
resource:com/paterva/maltego/java/config/jre/TestJDK.class → /tmp/temp13191485681352650521741683081305/TestJDK.class
executing: /usr/lib/jvm/jdk-11/bin/java -classpath /tmp/temp13191485681352650521741683081305 TestJDK, in: .
result: 0
command execution finished
out: 11.0.14, 11.0.14+8-LTS-263, Oracle Corporation, Linux, amd64
jdkHome: /usr/lib/jvm/jdk-11
canonical: /usr/lib/jvm/jdk-11
javaHome: /usr/lib/jvm/jdk-11
executing: /usr/lib/jvm/jdk-11/bin/java -classpath /tmp/temp13191485681352650521741683081305 TestJDK, in: .
result: 0
command execution finished
out: 11.0.14, 11.0.14+8-LTS-263, Oracle Corporation, Linux, amd64
jdkHome: /usr/lib/jvm/jdk-11
canonical: /usr/lib/jvm/jdk-11
javaHome: /usr/lib/jvm/jdk-11
executing: /usr/lib/jvm/jdk-11/bin/java -classpath /tmp/temp13191485681352650521741683081305 TestJDK, in: .
result: 0
command execution finished
out: 11.0.14, 11.0.14+8-LTS-263, Oracle Corporation, Linux, amd64
jdkHome: /usr/lib/jvm/jdk-11
canonical: /usr/lib/jvm/jdk-11
javaHome: /usr/lib/jvm/jdk-11
executing: /usr/lib/jvm/jdk-11/bin/java -classpath /tmp/temp13191485681352650521741683081305 TestJDK, in: .
result: 0
command execution finished
out: 11.0.14, 11.0.14+8-LTS-263, Oracle Corporation, Linux, amd64
jdkHome: /usr/lib/jvm/jdk-11
canonical: /usr/lib/jvm/jdk-11
javaHome: /usr/lib/jvm/jdk-11
```

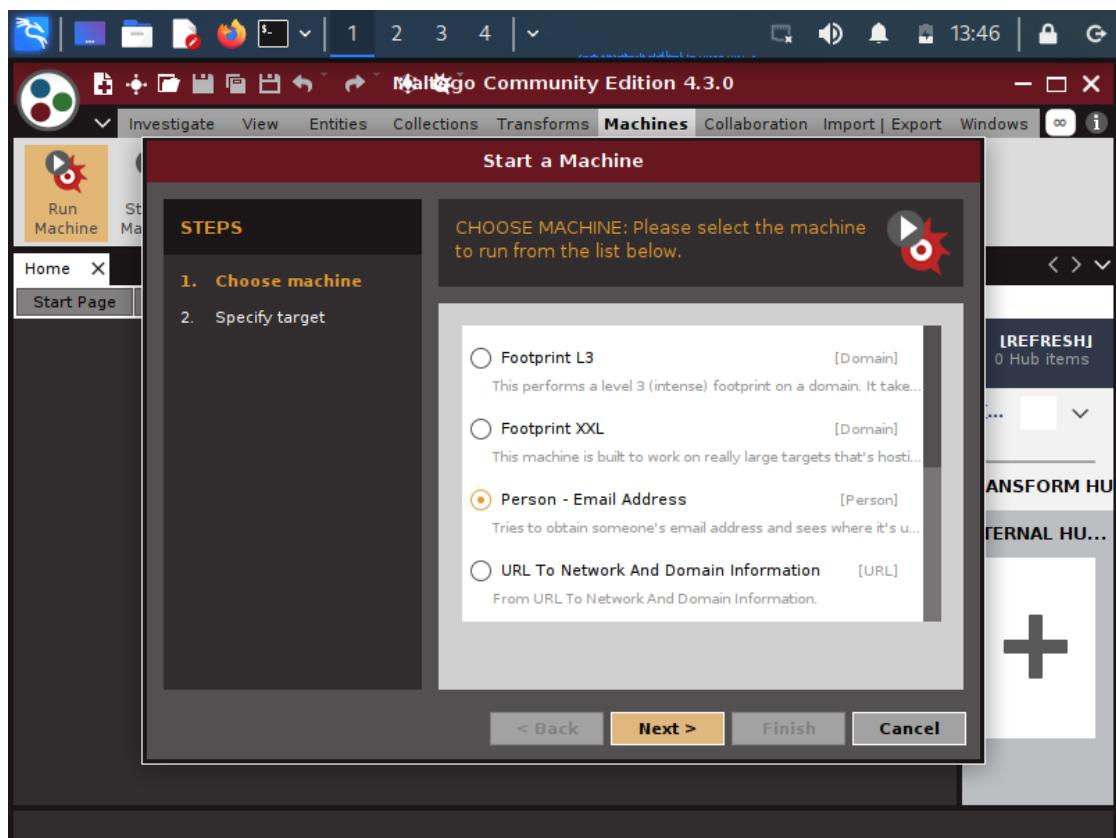
Register to Maltego by creating your account and login using the same credentials:
To login to the maltego, first We need to register on the website and fill in the requested details, then we can login to our maltego account.

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



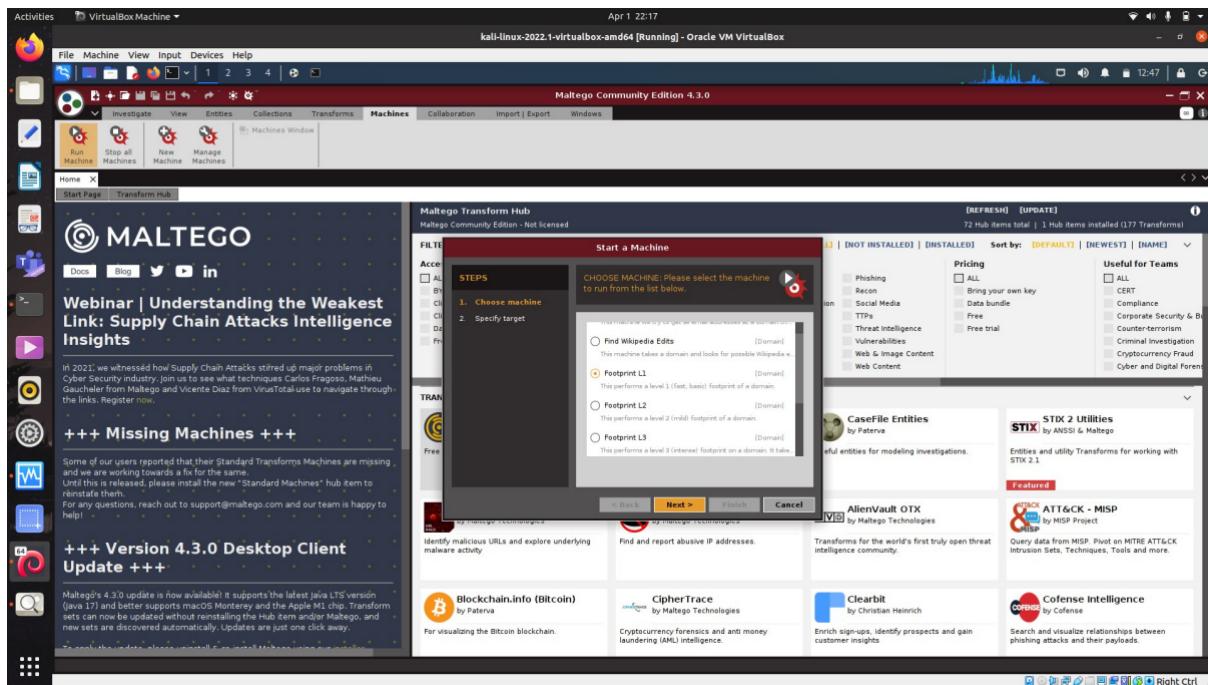
After you've set up your account, start the machine and select the type of reconnaissance you want to conduct on the target to link an email address to a person.

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.

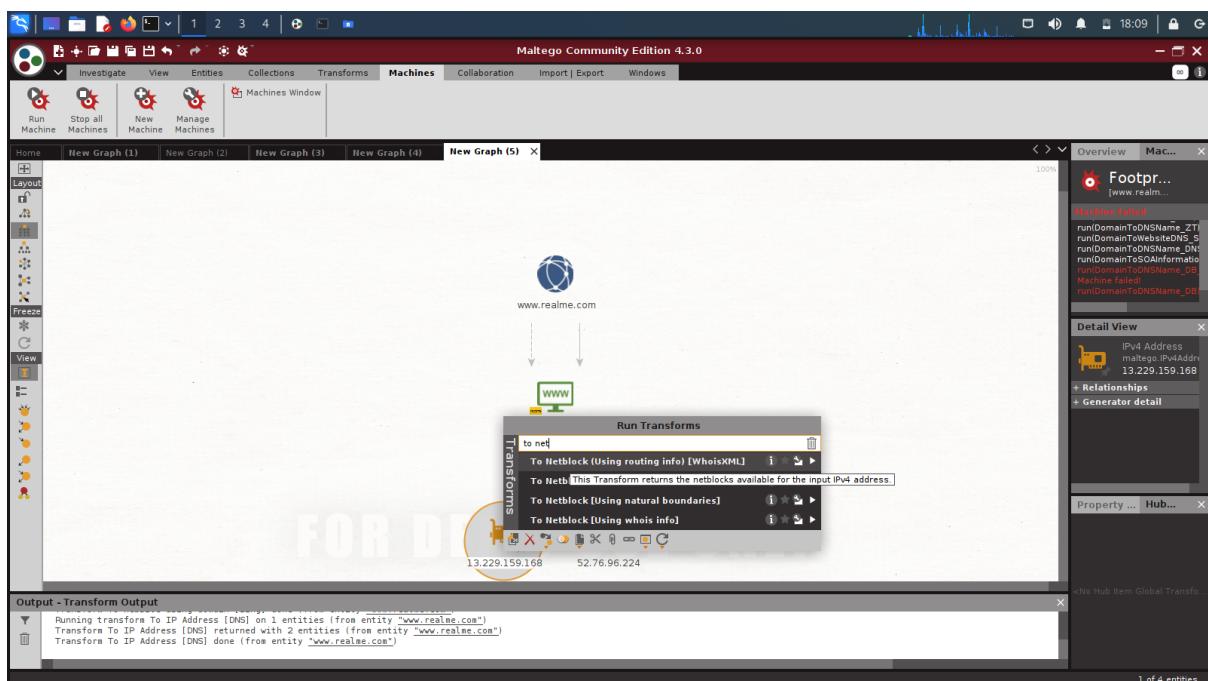
To link a website to a person, start a machine and select Footprint 1 from the type of reconnaissance menu. This is a basic footprint of a domain in its most basic form.

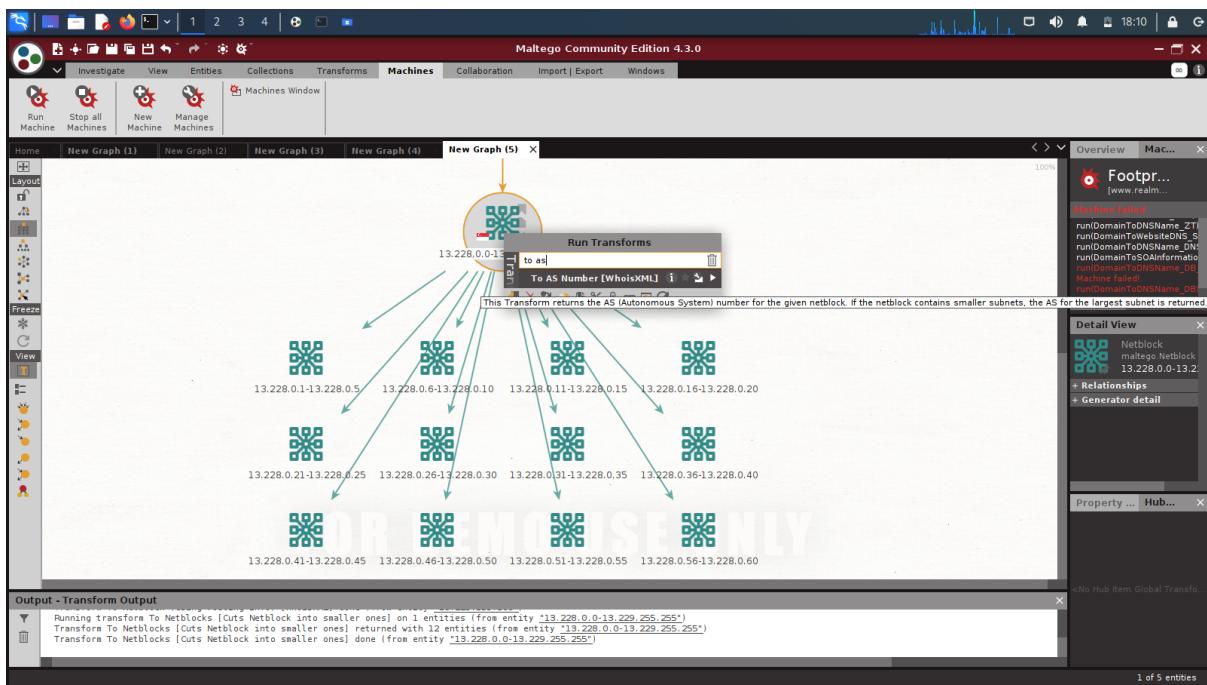
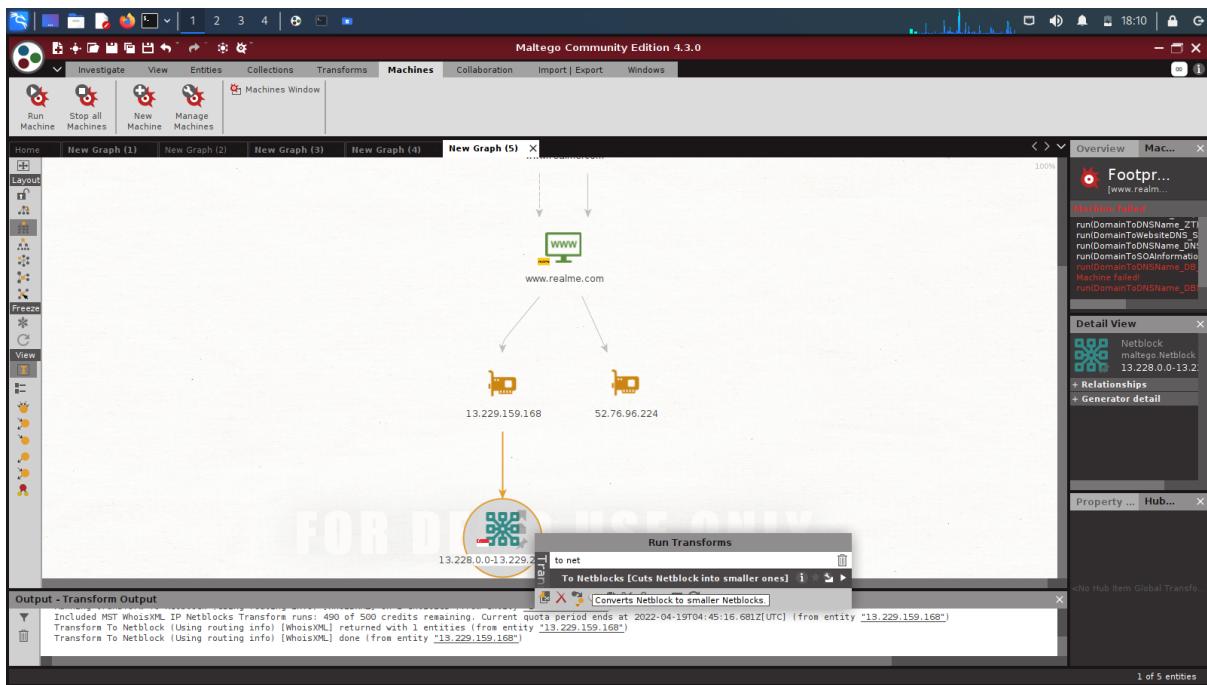


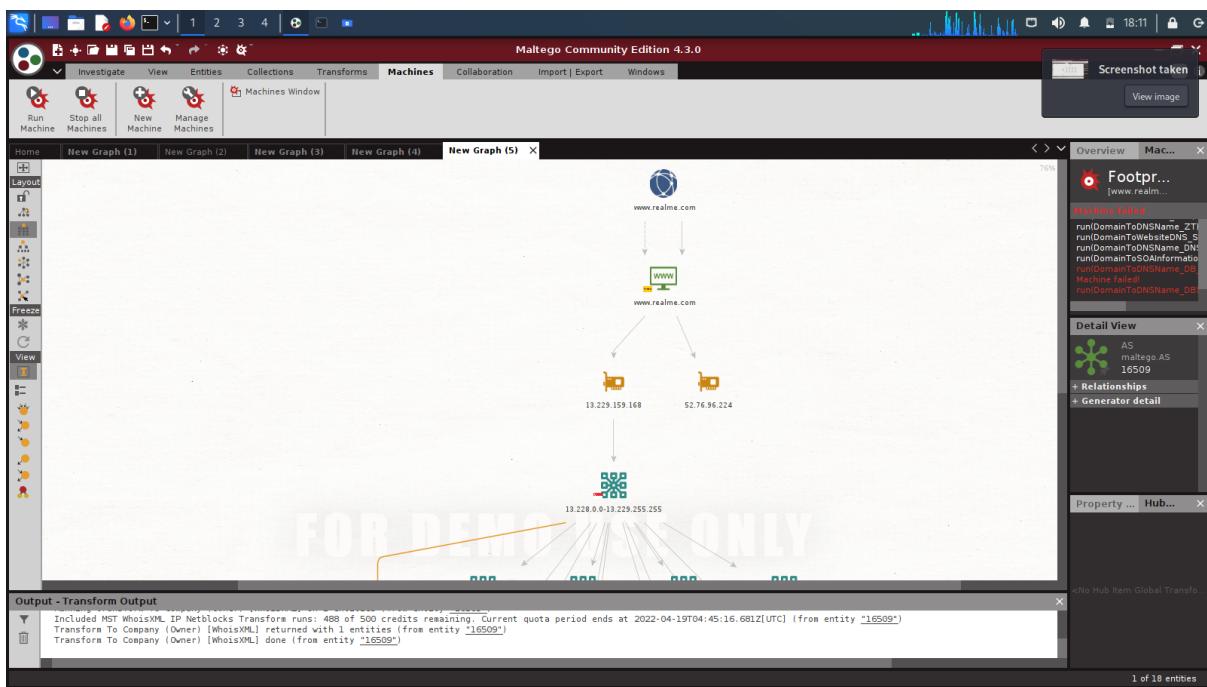
Let's us take a look of footprint on the website : www.realme.com

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.

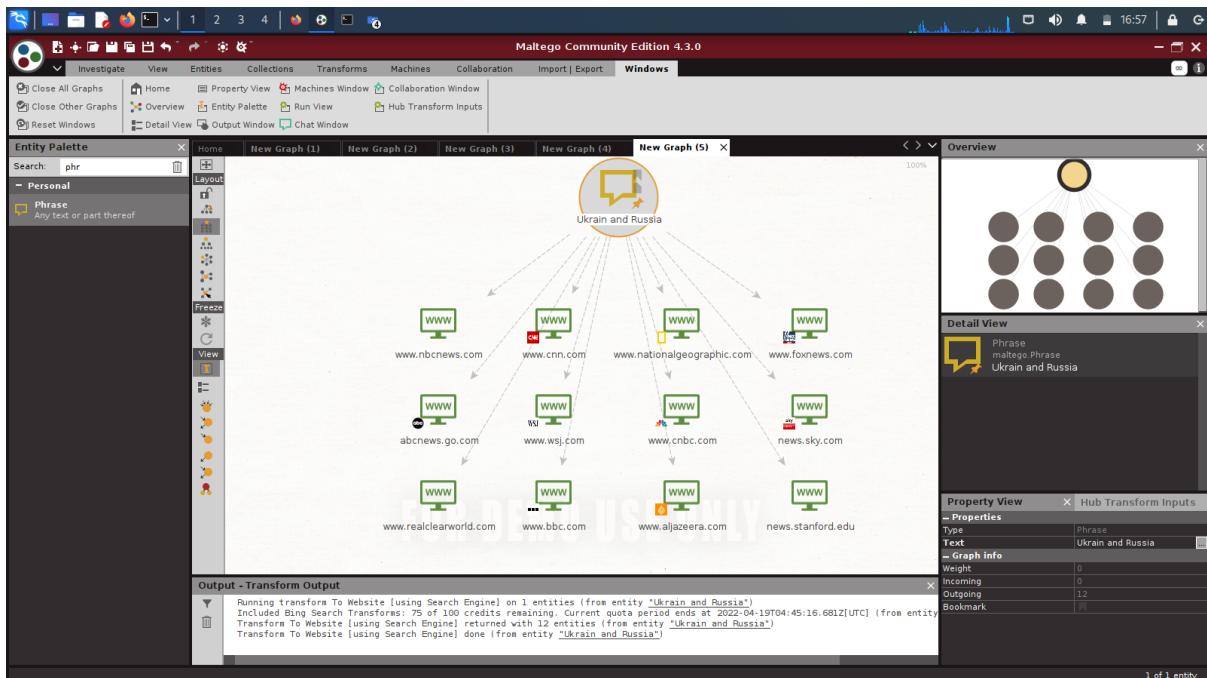


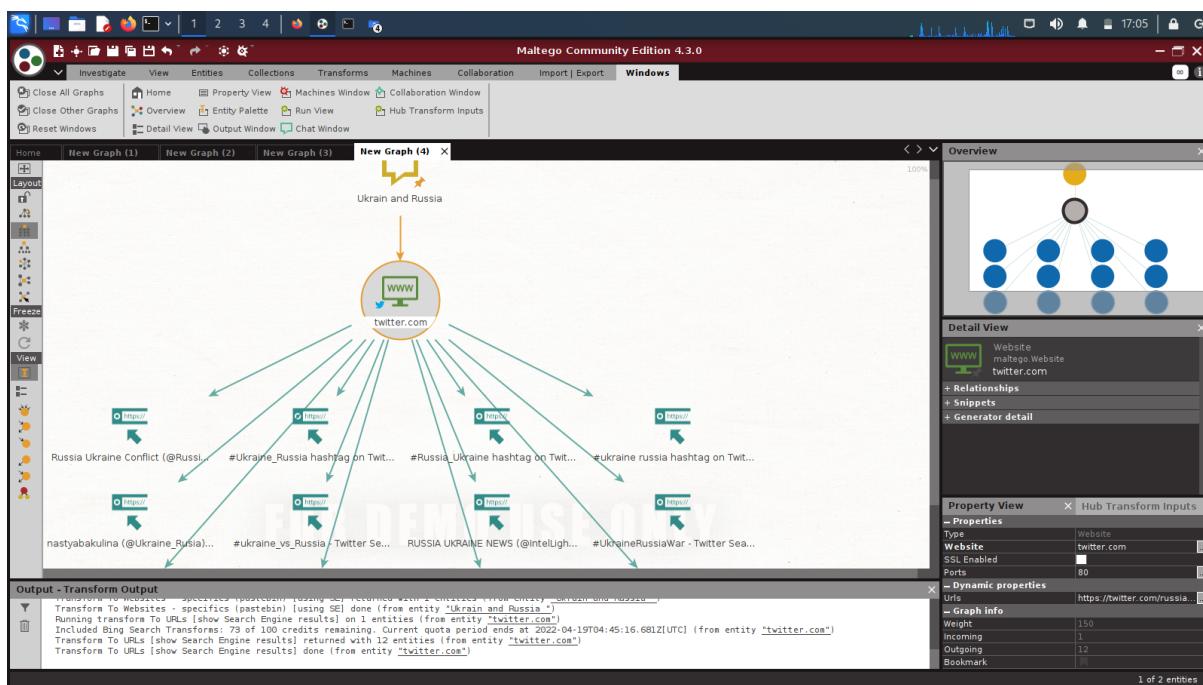
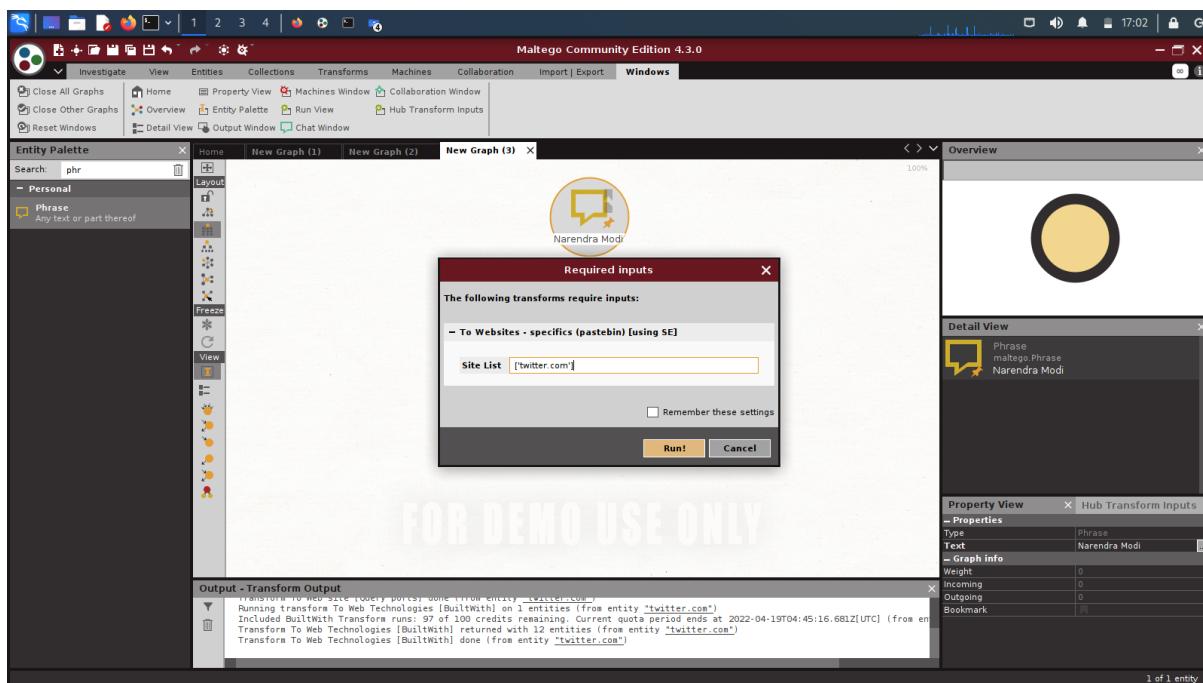




To verify an Email Address of a person drag and drop the email icon and right click on it to select the verify email transform. The output shows whether the email exists or not and returns an entity after verifying the address.

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.



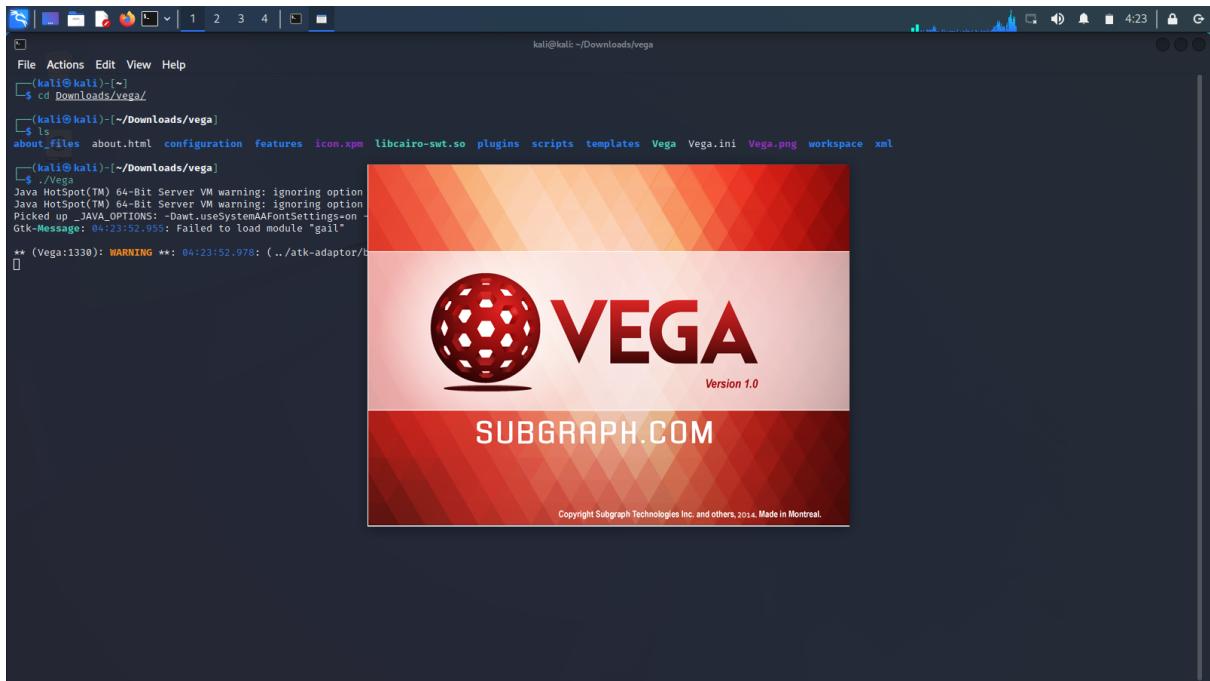


2. Vega

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’:

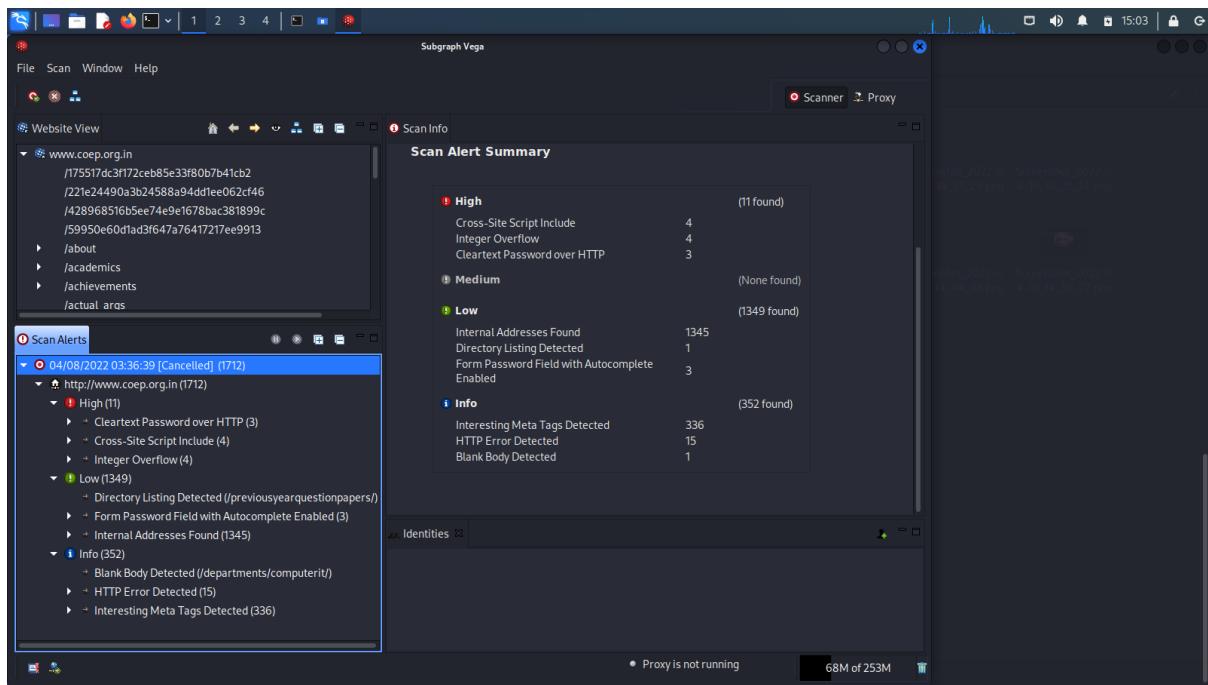


A screenshot of a terminal window on a Kali Linux desktop. The terminal shows the command `vega` being run, which starts the Vega application. The application's splash screen is displayed, featuring a red and orange geometric background with the word "VEGA" in large red letters, "Version 1.0" below it, and "SUBGRAPH.COM" at the bottom. The terminal also displays some Java warning messages about ignoring options and failed font loading.

```
kali㉿kali:~/Downloads/vega
File Actions Edit View Help
[kali㉿kali] ~
$ cd ~/Downloads/vega/
[kali㉿kali] ~/Downloads/vega
$ ls
about_files about.html configuration features icon.xpm libcairo-swt.so plugins scripts templates Vega Vega.ini Vega.png workspace xml
[kali㉿kali] ~/Downloads/vega
$ ./Vega
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option
picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on
Gtk-Message: 04-23:52.952: Failed to load module 'gail'
** (Vega:1330): WARNING **: 04:23:52.978: (.../atk-adaptor/)

Copyright Subgraph Technologies Inc. and others, 2014. Made in Montreal.
```

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.

```

File Actions Edit View Help
[kali㉿kali] ~
$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet 192.168.43.28 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopelen 0<link>
        inet6 2401:4980:1900:973b:2592:346d:7c40:484d prefixlen 64 scopelen 0<global>
            inet6 2401:4980:1900:973b:a00:27ff:fe95:bd54 prefixlen 64 scopelen 0<global>
                ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
                    RX packets 837 bytes 51820 (50.6 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 413 bytes 68980 (67.3 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopelen 0<link>
            loop txqueuelen 0 (Local Loopback)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[kali㉿kali] ~
* Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-10 14:23 EDT
Failed to resolve "0:0:0:27:95:bd:54".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

[kali㉿kali] ~
$ nmap -O 192.168.43.255
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-10 14:24 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.34 seconds

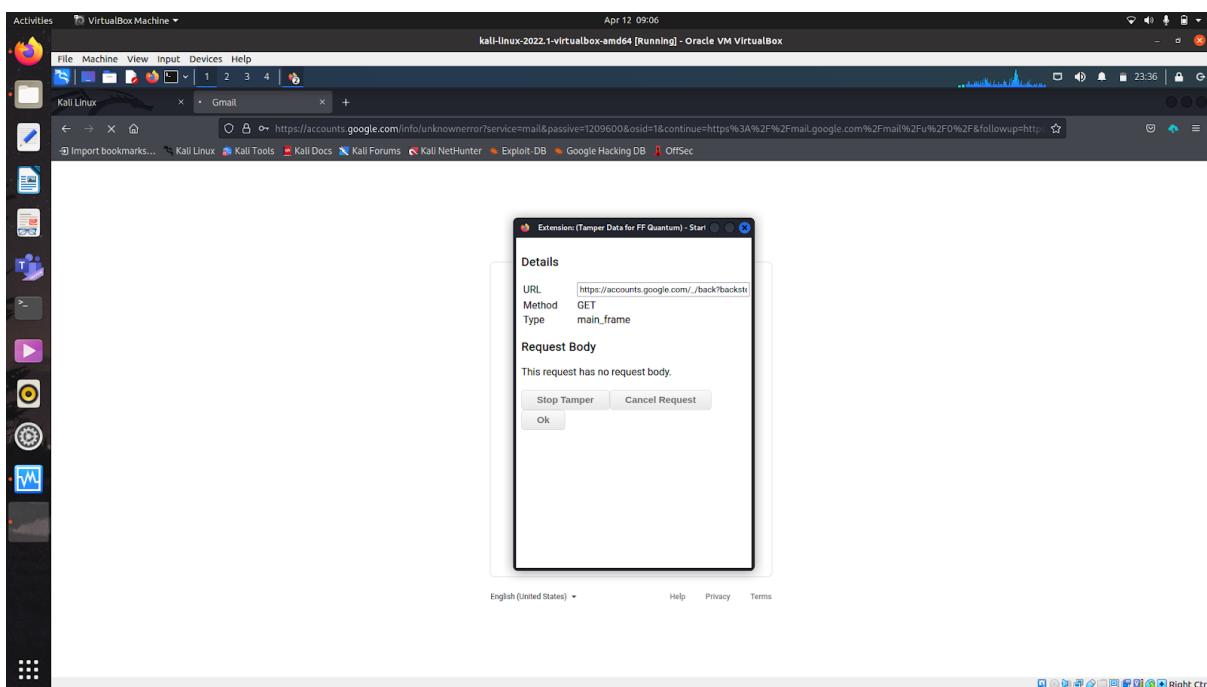
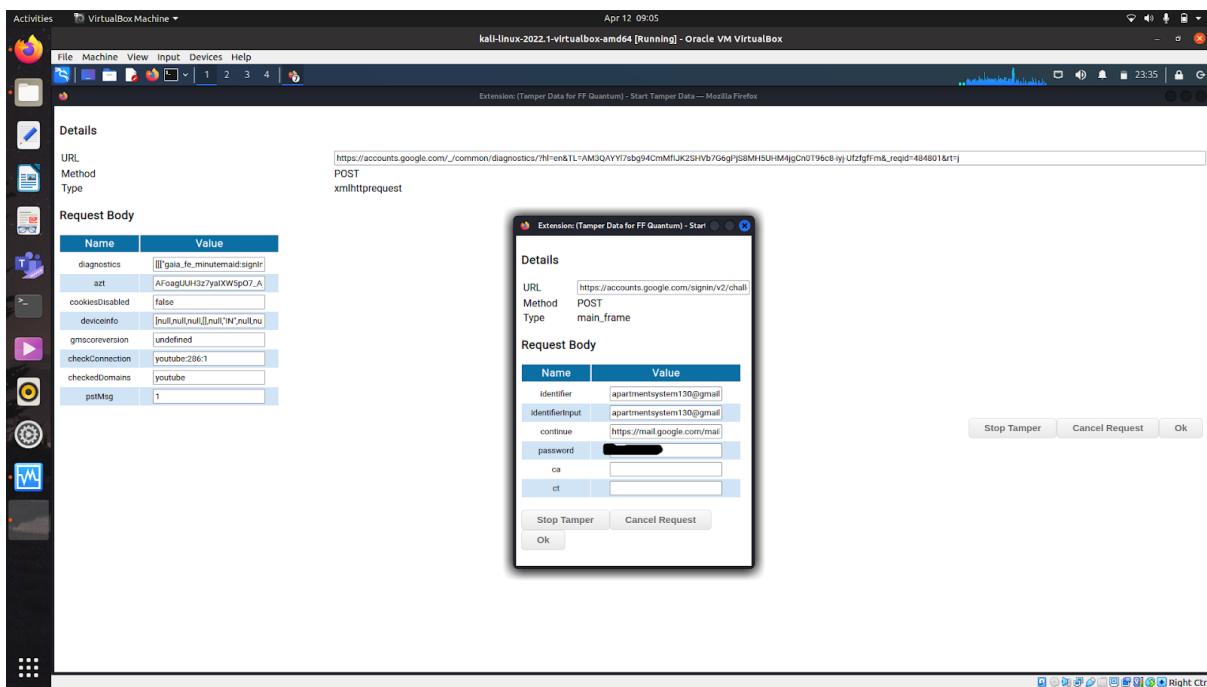
[kali㉿kali] ~
* Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-10 14:25 EDT
Nmap scan report for 192.168.43.1
Host is up (0.023s latency).
Nmap scan report for 192.168.43.27
Host is up (0.0036s latency).
Nmap scan report for 192.168.43.28
Host is up (0.00020s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.39 seconds

[kali㉿kali] ~
$ 

```

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.

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes	ibstat \$PATH Privilege Escalation
1	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes	Xorg X11 Server Local Privilege Escalation
2	exploit/aix/rpc_cmds_opcode21	2009-10-07	great	No	AIX Calendar Manager Service Daemon (rpc.cmds) OPCODE 21 Buffer Overflow
3	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No	ToolTalk rpc.ttdbserverd _t_internal_realpath Buffer Overflow (AIX)
4	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes	Android ADB Debug Server Remote Payload Execution
5	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	manual	No	Stagefright MP4 Tx3g Integer Overflow
7	exploit/android/browser/webview/addjavascriptinterface	2012-12-21	excellent	No	Android Browser and WebView addJavascriptInterface Code Execution
8	exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	No	Adobe Reader For Android addJavascriptInterface Exploit
9	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-Free Exploit
10	exploit/android/local/futex_requeue	2014-05-03	excellent	Yes	Android 'Towelroot' Futex Requeue Kernel Exploit
11	exploit/android/local/janus	2017-07-31	manual	No	Android Janus APK Signature bypass
12	exploit/android/local/user_vroot	2013-08-06	excellent	No	Android getuid/geteuid Exploit
13	exploit/android/local/su_exec	2017-08-31	manual	No	Android su ExecPrivilege Escalation
14	exploit/apple_ios/browser/safari_jit	2016-08-25	good	No	Safari Webkit JIT Exploit for iOS 7.1.2
15	exploit/apple_ios/browser/safari_libtiff	2006-08-01	good	No	Apple iOS MobileSafari LibTIFF Buffer Overflow

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

```

File Actions Edit View Help
msf6 > info exploit/apple_ios/browser/safari_jit
      Name: Safari Webkit JIT Exploit for iOS 7.1.2
      Module: exploit/apple_ios/browser/safari_jit
      Platform: Apple_iOS
      Arch: armle
      Privilaged: No
      License: Metasploit Framework License (BSD)
      Rank: Good
      Disclosed: 2016-08-25

Provided by:
kudima
Ian Beer
WanderingGlitch
timwr

Available targets:
Id Name
— —
0 Automatic

Check supported:
No

Basic options:
Name Current Setting Required Description
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert / no Path to a custom SSL certificate (default is randomly generated)
URI PATH / yes The URL to use for this exploit.

Payload information:

Description:
This module exploits a JIT optimization bug in Safari Webkit. This allows to write shellcode to an RWX memory section in JavaScriptCore and execute it. The shellcode contains a kernel exploit (CVE-2016-4669) that obtains kernel rw, obtains root and disables code signing. Finally we download and execute the meterpreter payload. This module has been tested against iOS 7.1.2 on an iPhone 4.

References:
https://nvd.nist.gov/vuln/detail/CVE-2016-4669
https://nvd.nist.gov/vuln/detail/CVE-2018-4162
https://github.com/kudima/exploit_playground/tree/master/iPhone3_1_shell

```

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

```

Activities VirtualBox Machine ▾
File Machine View Input Devices Help
File Actions Edit View Help
msf6 > info exploit/linux/http/mutiny_frontend_upload
      Name: Mutiny 5 Arbitrary File Upload
      Module: exploit/linux/http/mutiny_frontend_upload
      Platform: Linux
      Arch: x86
      Privilaged: Yes
      License: Metasploit Framework License (BSD) Windows
      Rank: Excellent
      Disclosed: 2013-05-15

Provided by:
juan vazquez <juan.vazquez@metasploit.com> description
File size Download
— —
0 Mutiny 5.0-1.07 Appliance (Linux) 172.62 MB https://download.oracle.com/java/10/jdk/jdk-10_linux-x64_bin.tar.gz [sha256:07]
Check supported: Arm 64 RPM Package 154.1 MB https://download.oracle.com/java/10/jdk/jdk-10_linux-x64_bin.rpm [sha256:07]

Basic options:
Name Current Setting Required Description
PASSWORD password yes The password to authenticate with
Proxies no no A proxy chain of format type:host:port][type:host:port][...
RHOSTS yes yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT 80 yes yes The port to connect to
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / yes Path to Mutiny Web Service
USERNAME superadmin@mutiny.com yes The user to log in as
VHOST no HTTP server virtual host

Payload information:

Description:
This module exploits a code execution flaw in the Mutiny 5 appliance. The EditDocument servlet provides a file upload function to authenticated users. A directory traversal vulnerability in the same functionality allows for arbitrary file upload, which results in a code execution. This module can be used to upload a file and exploit the vulnerability a valid user (any role) in the web frontend is required. The module has been tested successfully on the Mutiny 5.0-1.07 appliance.

References:
https://nvd.nist.gov/vuln/detail/CVE-2013-0136
OSVDB-9344
https://www.kb.cert.org/vuls/id/701572
https://blog.rapid7.com/2013/05/15/new-1day-exploits-mutiny-vulnerabilities

```

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.



