

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 identifiable. With 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

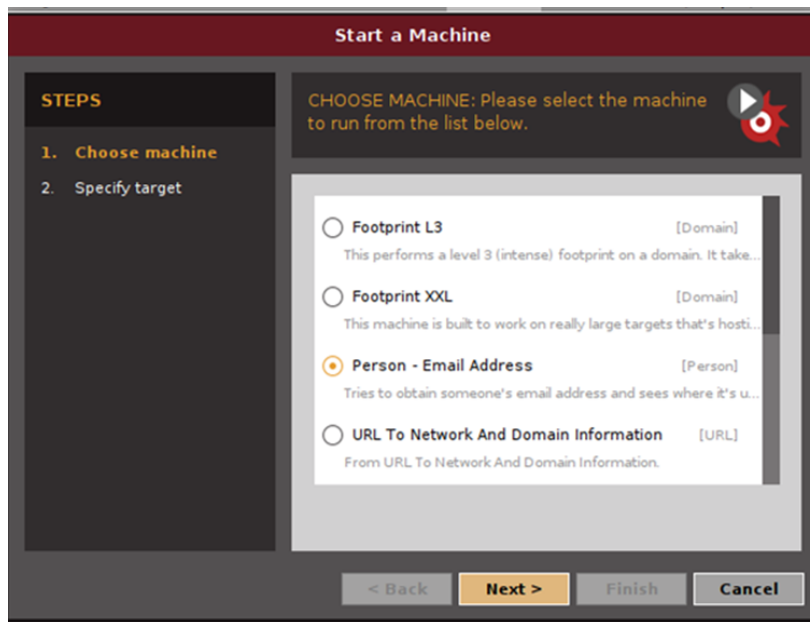
Step 3: Start a Machine

Step 4: Choose a target

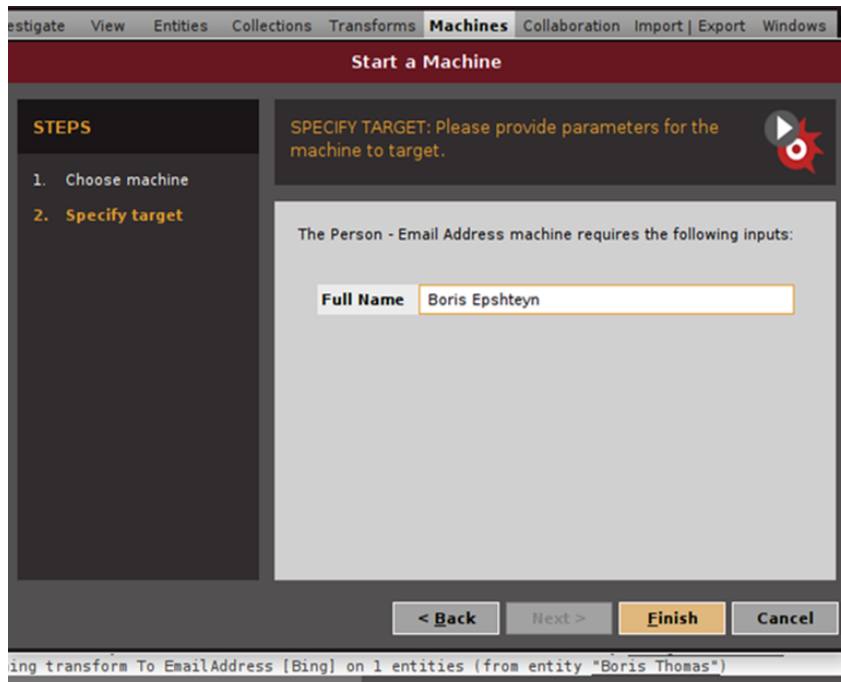
Step 5: Select the Appropriate Email Address

Step 6: Create a Graph of the Target

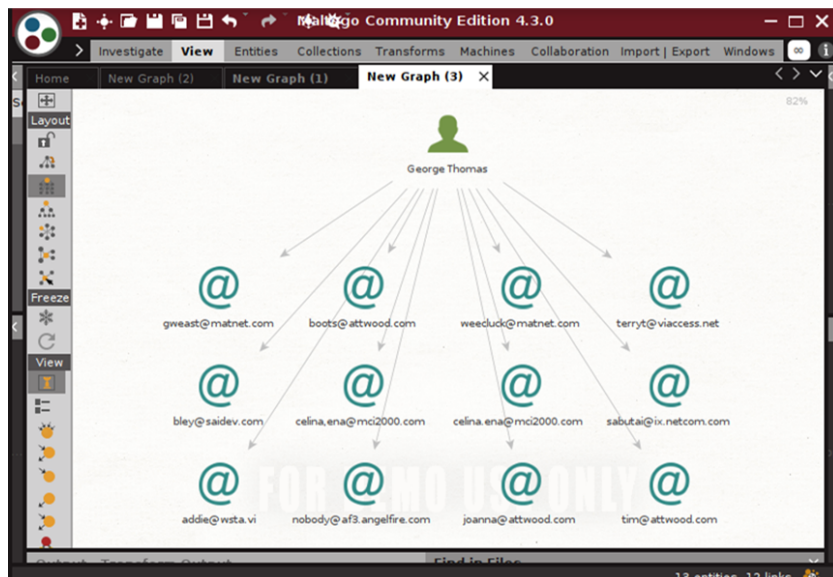
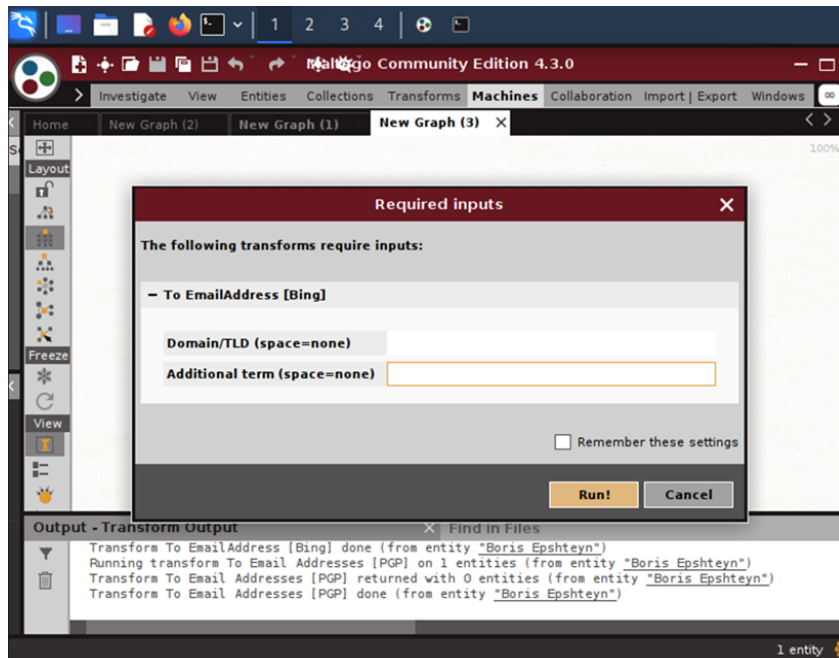
1. Associate an email to a person.



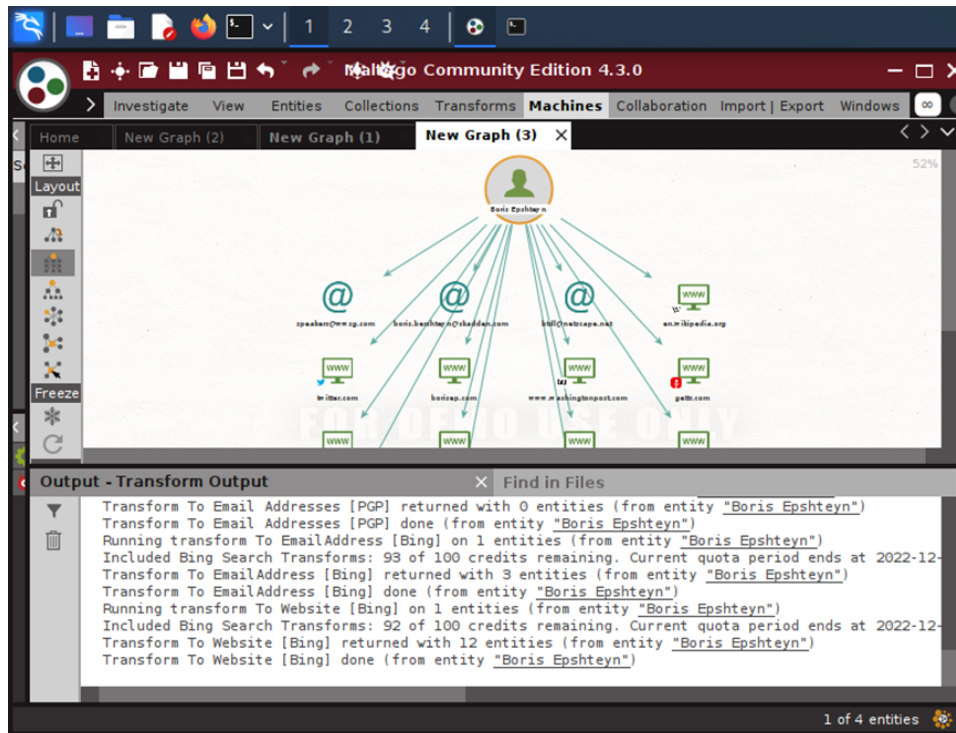
2. After you've set up your account, start the machine and select the type of reconnaissance you want to conduct on the target to link an email address to a person.(as per above diagram).



- 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.



- 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

```

L$ 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

```

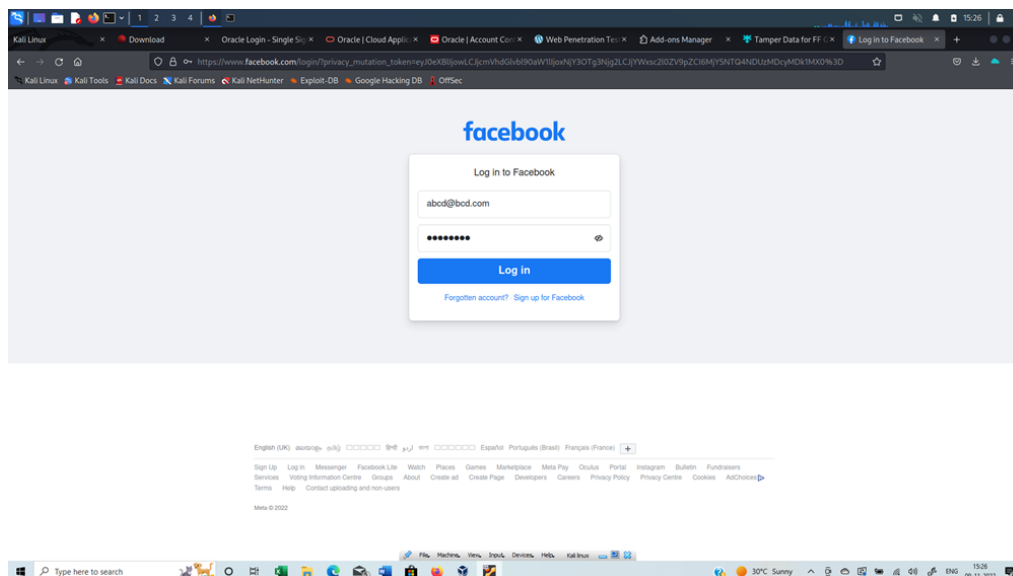
- **Tamper Data Plugin**

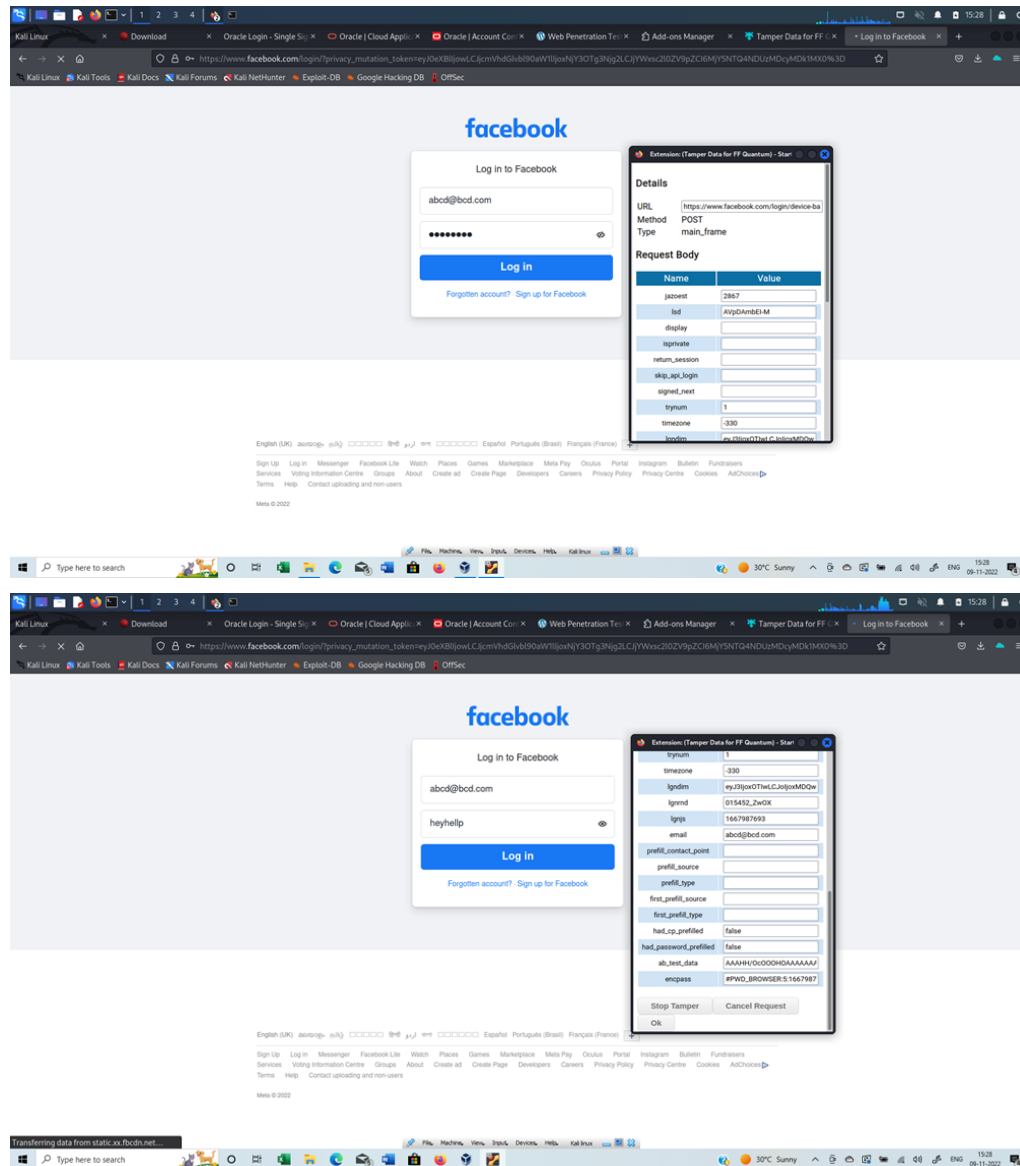
Tampering is the way of modifying the request parameters before request submission. Tampering can be achieved by various methods and one of the ways is through Tamper Data. Tamper data is one of the highly used extensions in Firefox. It allows tampering of the data that is sent between the client and 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





- **Metasploit Exploits**

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.

kali > show exploits

Exploits

#	Name	Description	Disclosure Date	Rank
0	exploit/aix/local/ibstat_path		2013-09-24	exce
1	exploit/aix/local/ibstat_privilege_escalation		2018-10-25	grea
2	exploit/aix/local/ibstat_privilege_escalation		2018-10-25	grea
3	exploit/aix/rpc/ttdserverd_realpath		2009-06-17	grea
4	exploit/android/adb/adb_server_exec		2016-01-01	exce
5	exploit/android/browser/samsung_knox_smds_url		2014-11-12	exce
6	exploit/android/browser/stagefright_mp3_t3g_64bit		2015-08-13	norm
7	exploit/android/browser/webview_addjavascriptinterface		2012-12-21	exce
8	exploit/android/fileformat/adobe_reader_pdf_js_interface		2014-04-13	good
9	exploit/android/local/binder_uaf		2019-09-26	exce
10	exploit/android/local/futex_requeue		2014-05-03	exce
11	exploit/android/local/janus		2017-07-31	manu
12	exploit/android/local/put_user_vroot		2013-09-06	exce
13	exploit/android/local/su_exec		2017-08-31	manu
14	exploit/apple_ios/browser/safari_jit		2016-08-25	good
15	exploit/apple_ios/browser/safari_libtiff		2016-08-25	good
16	exploit/apple_ios/browser/webkit_createthis		2016-08-25	manu
17	exploit/apple_ios/browser/webkit_trident		2016-08-25	manu
18	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
19	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
20	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
21	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
22	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
23	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
24	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
25	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
26	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
27	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
28	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
29	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
30	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
31	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
32	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
33	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
34	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
35	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
36	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
37	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
38	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
39	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
40	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
41	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
42	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
43	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
44	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
45	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
46	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
47	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
48	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
49	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
50	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
51	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
52	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
53	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
54	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
55	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
56	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
57	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
58	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
59	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
60	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
61	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
62	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
63	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
64	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
65	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
66	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
67	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
68	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
69	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
70	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
71	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
72	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
73	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
74	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
75	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
76	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
77	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
78	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
79	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
80	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
81	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
82	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
83	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
84	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
85	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
86	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
87	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
88	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
89	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
90	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
91	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
92	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
93	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
94	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
95	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
96	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
97	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
98	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good
99	exploit/apple_ios/email/mobilemail_libtiff		2016-08-25	good

These are the available Exploits in Kali Linux.