**Recon-ng – advanced reconnaissance framework**



*My buddy Aamir Lakhani wrote about a cool reconnaissance tool called recon-ng. This tool can automate researching a target using multiple sources. The original post can be found* [*HERE.*](http://www.drchaos.com/recon-ng-advanced-reconnaissance-framework/)Reconnaissance techniques are the one of the first steps penetration testers practice when learning how to exploit systems for vulnerabilities. Traditional reconnaissance techniques are used to gather intelligence, define scope, and identifying weaknesses.

The issue with reconnaissance is that is takes it time. In most cases, penetration testers do not have the luxury of time that at motivated attacker is going to have. I cannot stress the importance of reconnaissance. However, if you assume over a long period of time attackers will be able to gather intelligence, then methods such as credential white box penetration testing starts to make sense. Recon-ng is a tool that allows penetration testers to speed up advanced reconnaissance.

>Recon-ng is a framework. It is a very powerful, flexible, and has moving parts similar to the

Metasploit framework. Recon-ng is an interactive framework that is not a menu driven UI.

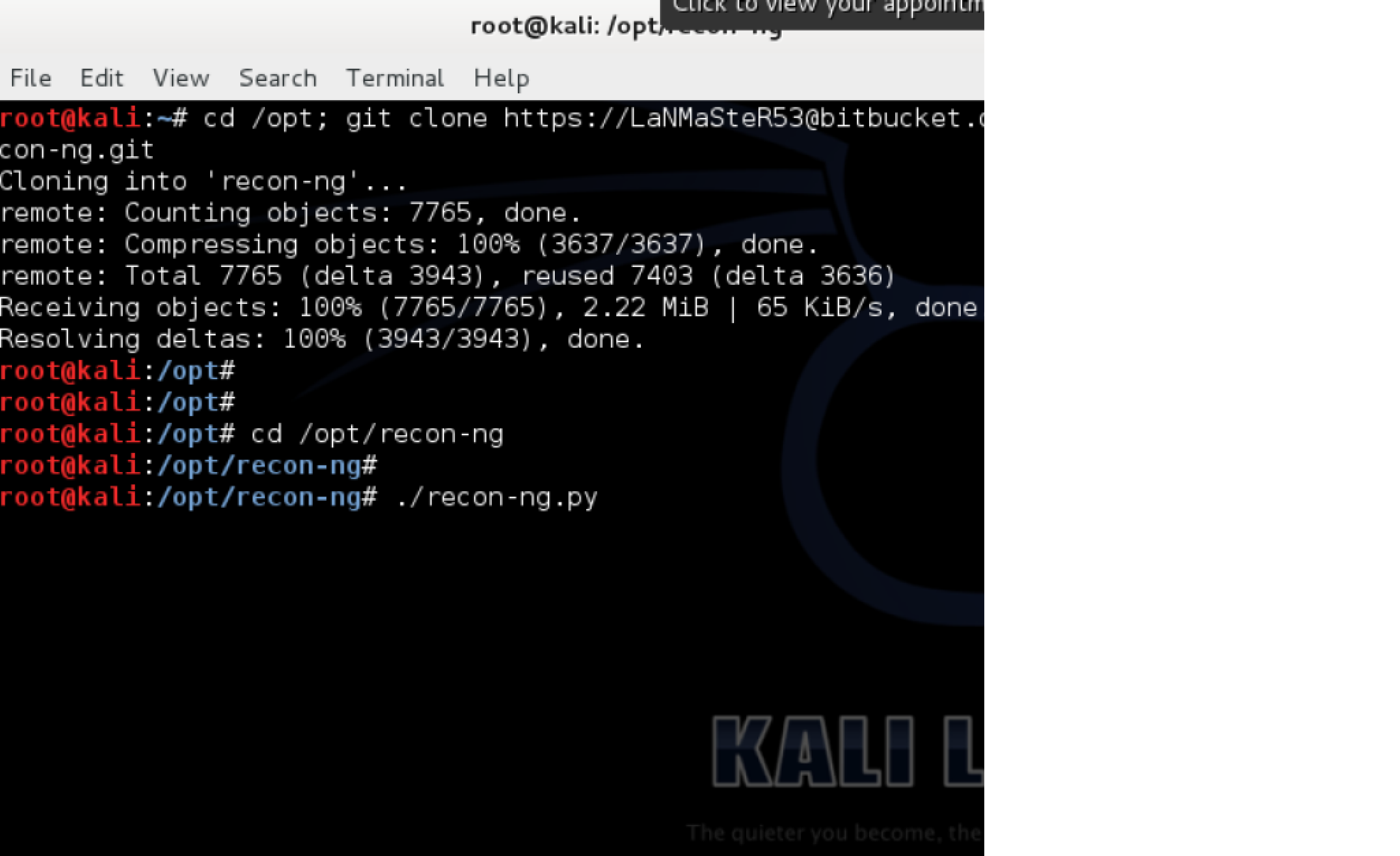
Recon-ng uses many different sources to gather data. Some of these sources are Google, Twitter, and Showdan. Some of these modules require paid APIs (other APIs are free, and some Recon- ng modules require no APIs).

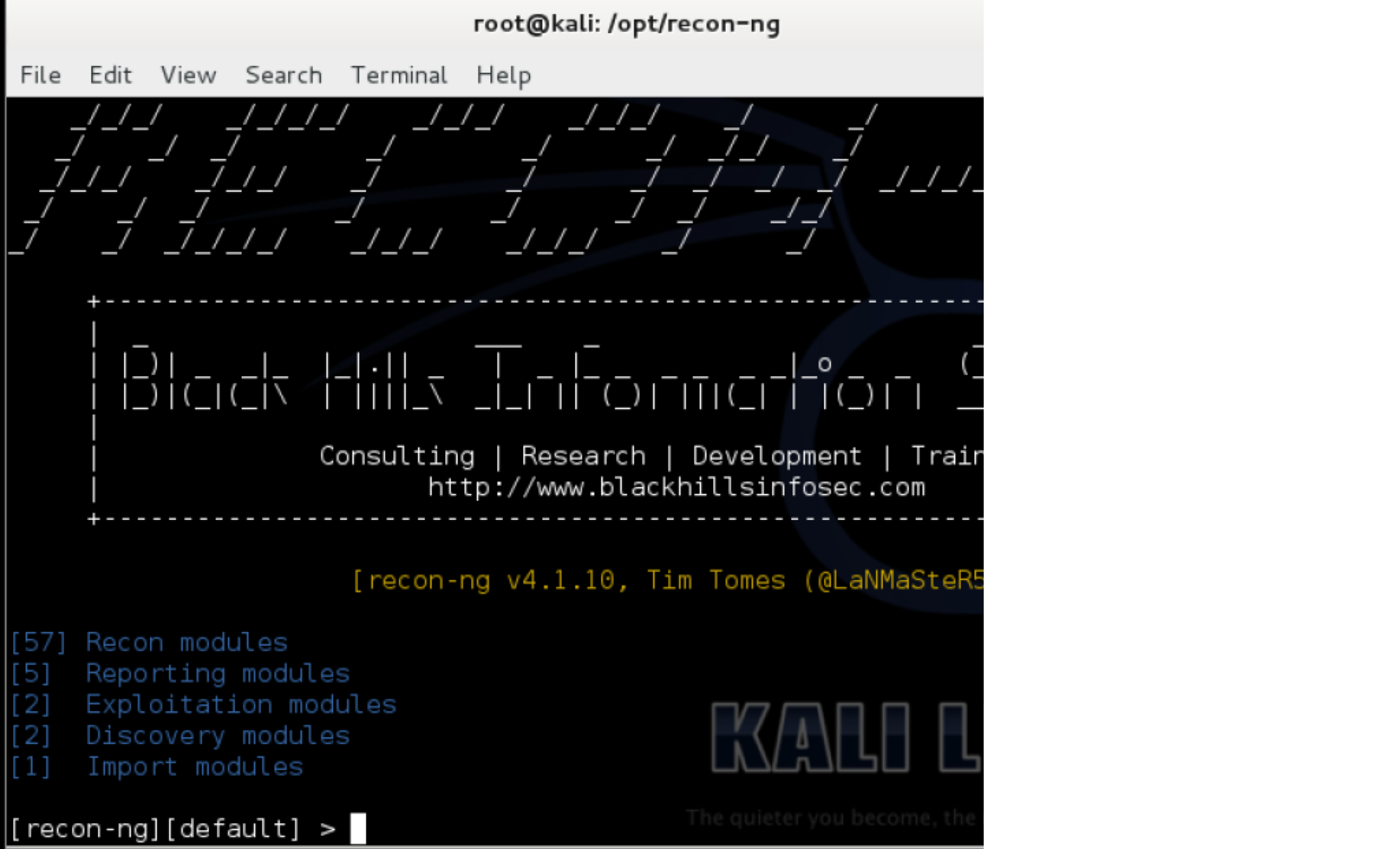
**Installing recon-ng on Kali Linux**

We are going to install recon-ng on Kali Linux. To install recon-ng and place it in the opt directory, we are going to use git clone by typing in the following command in the terminal window.

*cd /opt; git clone https:/*[*/LaNMaSteR53@bitbucket.org*](mailto:LaNMaSteR53@bitbucket.org)*/LaNMaSteR53/recon-ng.git cd /opt/recon-ng*

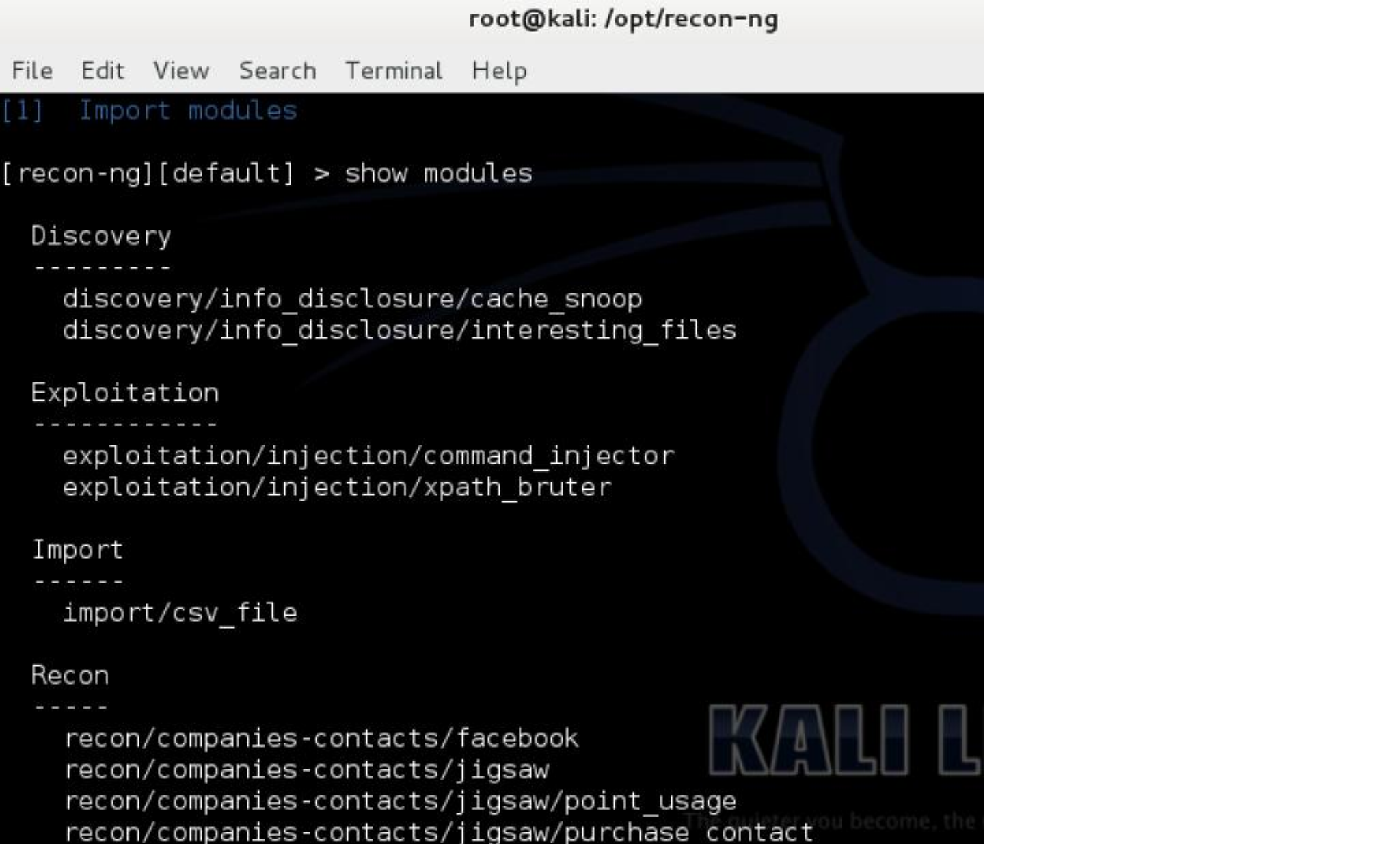
./recon-ng



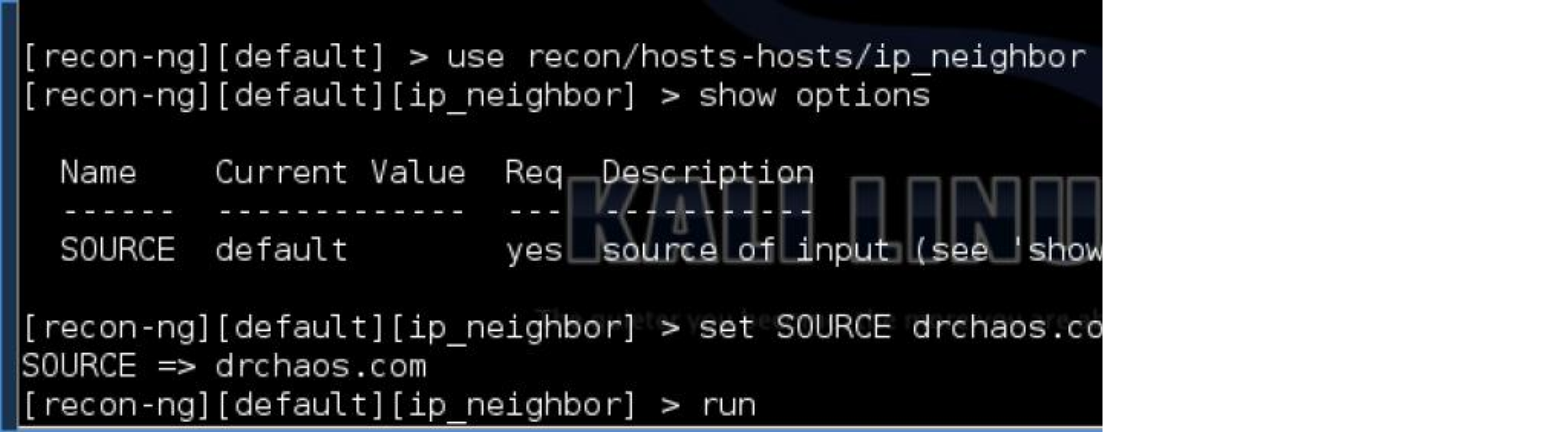


Recon-ng is an open-source framework coded in python by Tim Tomes a.k.a LaNMaSteR53. Its interface is modeled after the look of the Metasploit Framework but it is not for exploitation or for spawning a meterpreter session or a shell, it is for web-based reconnaissance and information gathering. It is not a menu driven UI. Do not type numbers. Use commands or type **help**.

It comes with modules to support your web reconnaissance adventure and information gathering just like Metasploit’s auxiliary and exploit modules. The modules pre-loaded for this framework are categorized into Auxiliary, Contacts, Hosts, Output, and Pwnedlist module types.



[My-IP-Neighbors Lookup is a recon module contributed by Micah Hoffman which checks and leverages my-ip-neighbors.com site for other hosts hosted on the same server. This is useful](http://www.thesecurityblogger.com/recon-ng-advanced-reconnaissance-framework/show-modules-recon-ng-1024x617/) [because it let’s you discovery relationships. It is possible your target hosts website could](http://www.thesecurityblogger.com/recon-ng-advanced-reconnaissance-framework/show-modules-recon-ng-1024x617/) be [hosted on a shared system with other sites that have vulnerabilities or exploits. In the following example we see DrChaos.com web server shares the same server with any other hosts.](http://www.thesecurityblogger.com/recon-ng-advanced-reconnaissance-framework/show-modules-recon-ng-1024x617/)



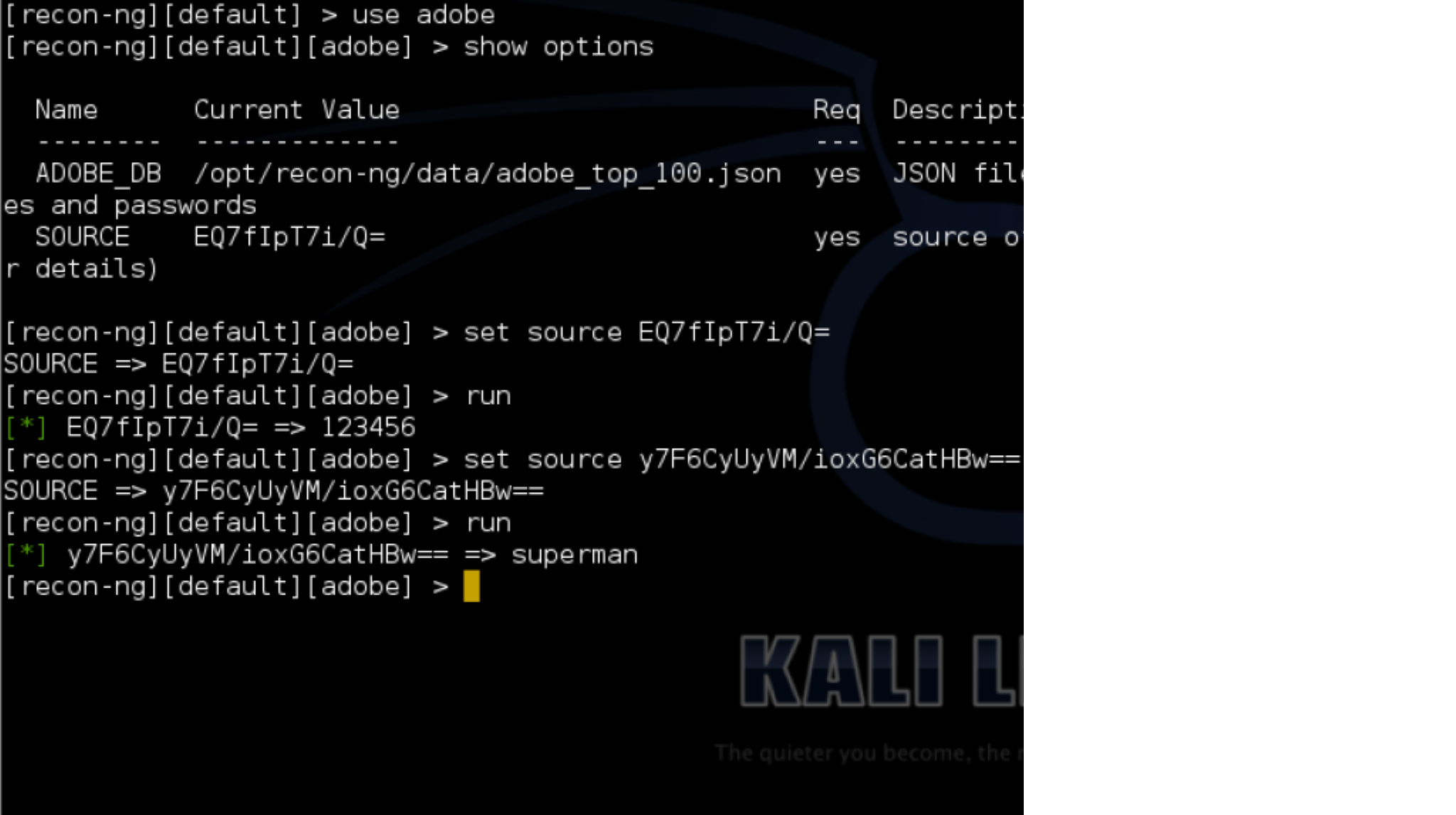
[Okay, my web host has me on the same server as revenge.info and boobzworld.com and](http://www.thesecurityblogger.com/recon-ng-advanced-reconnaissance-framework/show-modules-recon-ng-1024x617/)



Other types of common reconnaissance methods include: Whois

Google Adsense

Search Engine

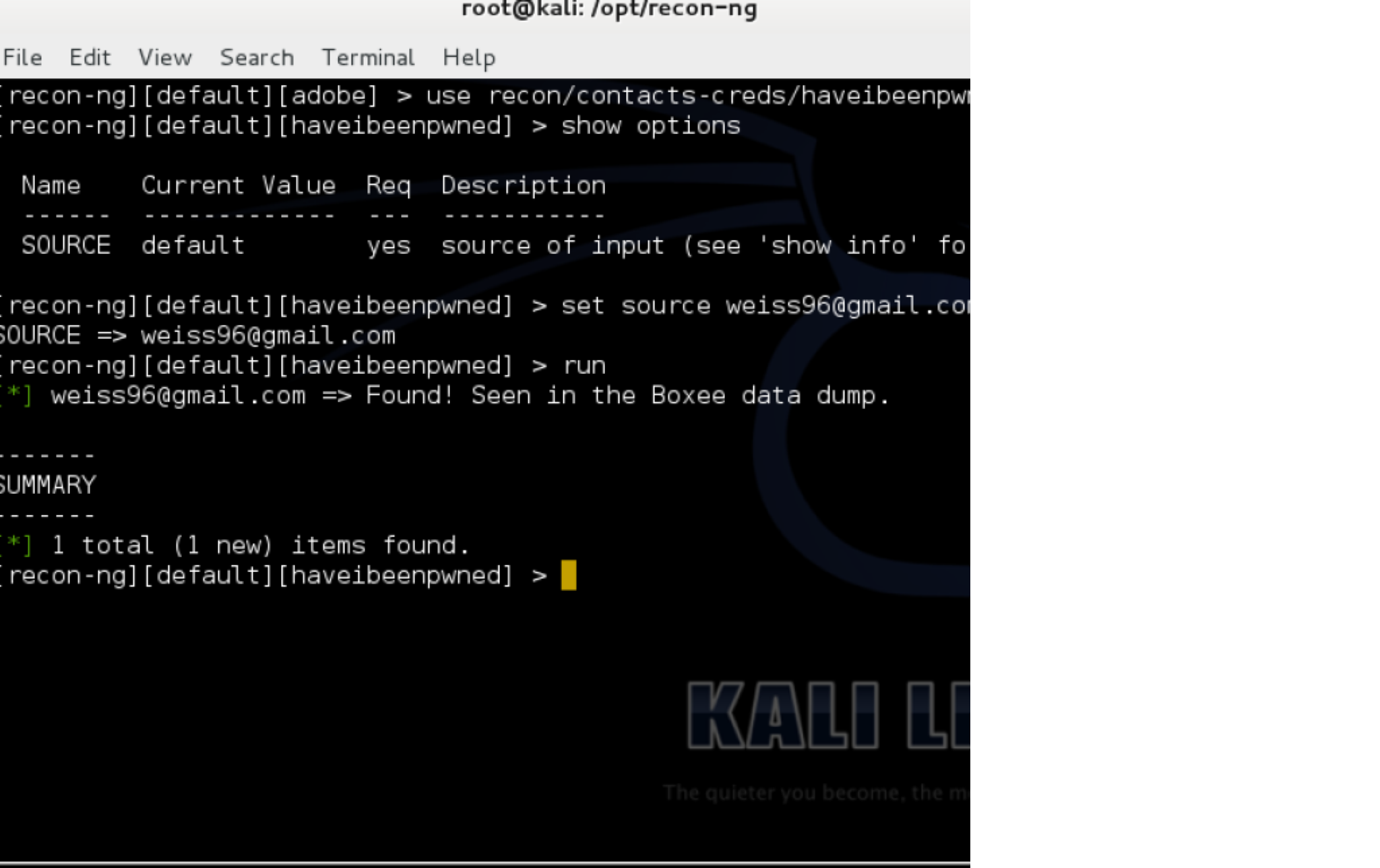


Geolocation.

In the next module we will take password hashes and see if we can match them against the Adobe password breach. This assumes we have password hashes that can be checked against the Adobe leaked hashes.

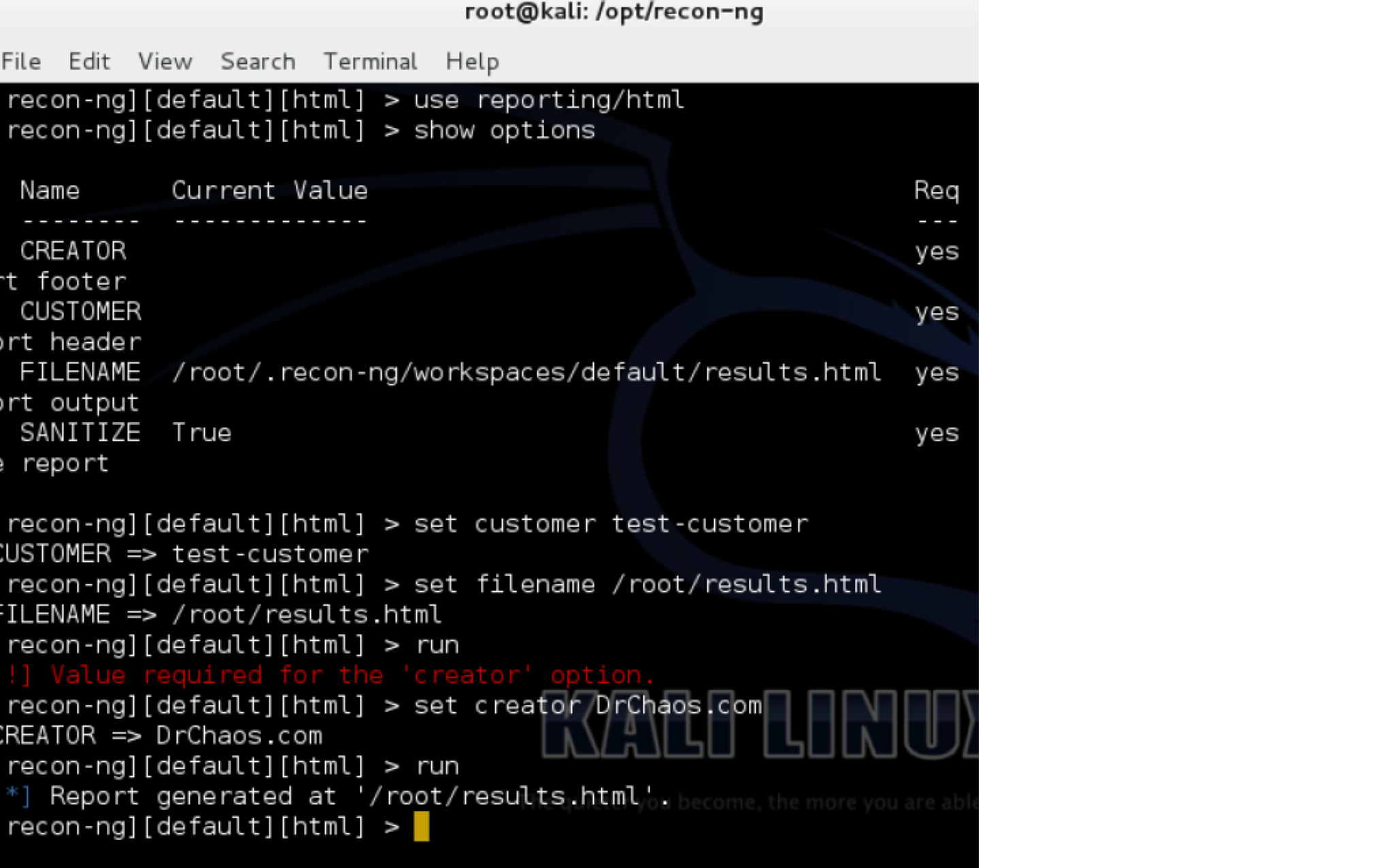
You can see from the example above our first hash was for the password 123456. Our second hash was for the password superman.

Now we will use the *Have I Been Pwned Module* to check if any user names we may have are compromised from any publicly known breaches.



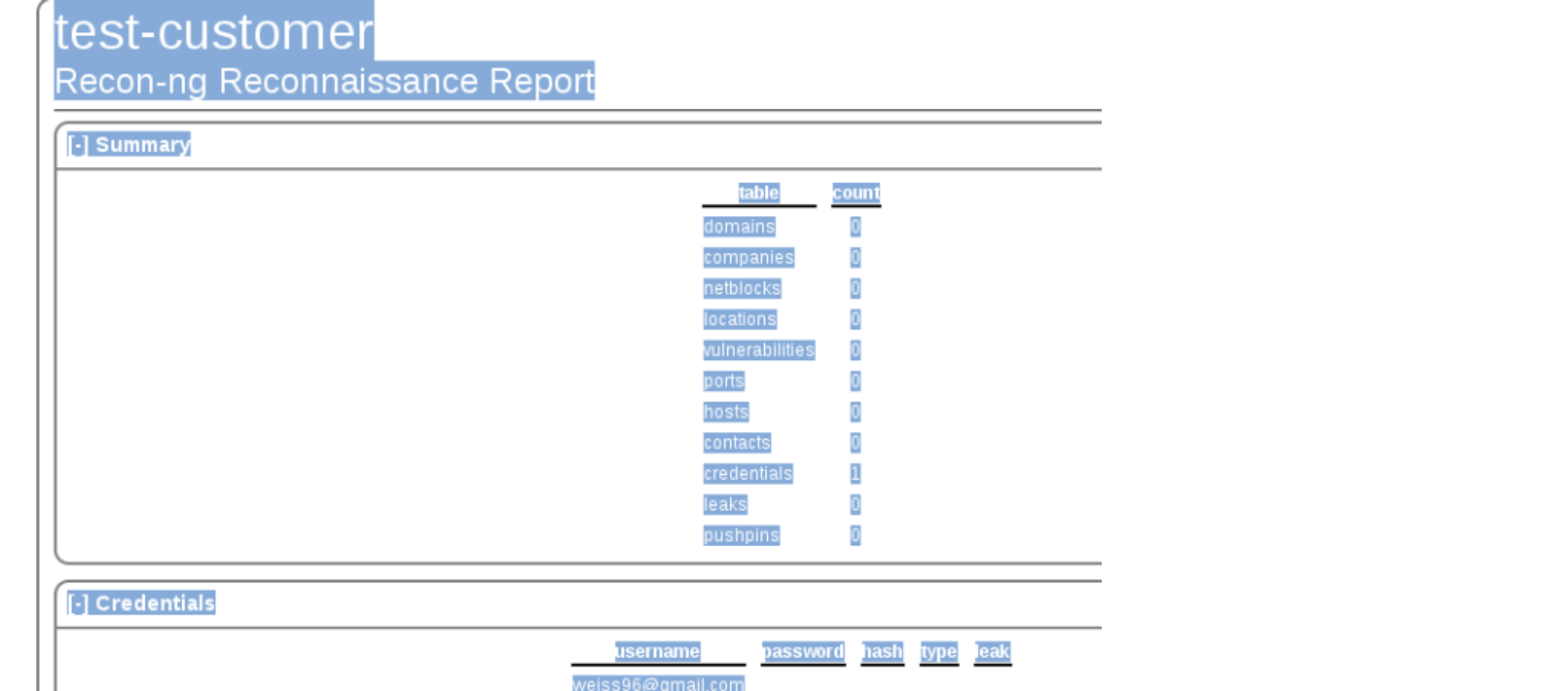
We can see the username [weiss96@gmail.com](mailto:weiss96@gmail.com) was breached from Boxee. If I knew this user’s hash or password, I could see if they had used it anywhere else. This type of reconnaissance is one of the strengths of recon-ng. You will in most instances need to use multiple modules to get the information you want.

Lastly, recon-ng puts all the information in learns into nice exportable reports.



There is not much in this report, but when you start running multiple modules and add in geolocation reports can get pretty complex, and recon-ng does a great job keeping track of everything.







[Recon-ng is a great framework to start your research. You will need to use multiple modules together to make a bigger picture and gather useable intelligence. Many of the modules require paid or free APIs.](http://www.thesecurityblogger.com/recon-ng-advanced-reconnaissance-framework/navigating-to-my-report-recon-ng-300x62/)

RECON-NG – ADVANCED RECONNAISSANCE FRAMEWORK

Reconnaissance techniques are the one of the first steps penetration testers learn when learning how to exploit systems for vulnerabilities. Traditional reconnaissance techniques are used to gather intelligence, define scope, and identifying weaknesses.

The issue with reconnaissance is that is takes it time. In most cases, penetration testers do not have the luxury of time that at motivated attacker is going to have. I cannot stress the importance of reconnaissance. However,

if you assume over a long period of time attackers will be able to gather intelligence, then methods such as credential white box penetration testing starts to make sense. Recon-ng is a tool that allows penetration testers to speed up advanced reconnaissance.

Recon-ng is a framework. It is a very powerful, flexible, and has moving parts similar to the Metasploit framework. Recon-ng is an interactive framework that is not a menu driven UI. Recon-ng uses many different

sources to gather data. Some of these sources use Google, Twitter, and Showdan. Some of these modules require paid APIs (other APIs are free, and some Recon-ng modules require no APIs).

Installing recon-ng on Kali Linux

We are going to install recon-ng on Kali Linux. To install recon-ng and place it in the opt directory, we are going to use git clone by typing in the following command in the terminal window.

cd /opt; git clone https:/[/LaNMaSteR53@bitbucket.org](mailto:LaNMaSteR53@bitbucket.org)/LaNMaSteR53/recon-ng.git cd /opt/recon-ng

./recon-ng

Recon-ng is an open-source framework coded in python by Tim Tomes a.k.a LaNMaSteR53. Its interface is modeled after the look of the Metasploit Framework but it is not for exploitation or for spawning a meterpreter session or a shell, it is for web-based reconnaissance and information gathering. It is not a menu driven UI. Do not type numbers. Use commands or type help.

It comes with modules to support your web reconnaissance adventure and information gathering just like

Metasploit’s auxiliary and exploit modules. The modules pre-loaded for this framework are categorized into

Auxiliary, Contacts, Hosts, Output, and Pwnedlist module types.

You can view the modules by typing show modules

My-IP-Neighbors Lookup is a recon module contributed by Micah Hoffman which checks and leverages my- ip-neighbors.com site for other hosts hosted on the same server. This is useful because it let’s you discovery relationships. It is possible your target hosts website could be hosted on a shared system with other sites that have vulnerabilities or exploits. In the following example we see DrChaos.com web server shares the same server with any other hosts.

Okay, my web host has me on the same server as revenge.info and boobzworld.com and scaledrop.com.

Other types of common reconnaissance methods include: Whois

Google Adsense

Search Engine DNS Brute force Geolocation.

In the next module we will take password hashes and see if we can match them against the Adobe password breach. This assumes we have password hashes that can be checked against the Adobe leaked hashes. You can see from the example above our first hash was for the password 123456. Our second hash was for the password superman.

Now we will use the Have I Been Pwned Module to check if any user names we may have are compromised from any publicly known breaches.

We can see the username [weiss96@gmail.com](mailto:weiss96@gmail.com) was breached from Boxee. If I knew this user’s hash or password, I could see if they had used it anywhere else. This type of reconnaissance is one of the strengths of recon-ng. You will in most instances need to use multiple modules to get the information you want.

Lastly, recon-ng puts all the information in learns into nice exportable reports.

There is not much in this report, but when you start running multiple modules and add in geolocation reports can get pretty complex, and recon-ng does a great job keeping track of everything.

Recon-ng is a great framework to start your research. You will need to use multiple modules together to make a bigger picture and gather useable intelligence. Many of the modules require paid or free APIs.