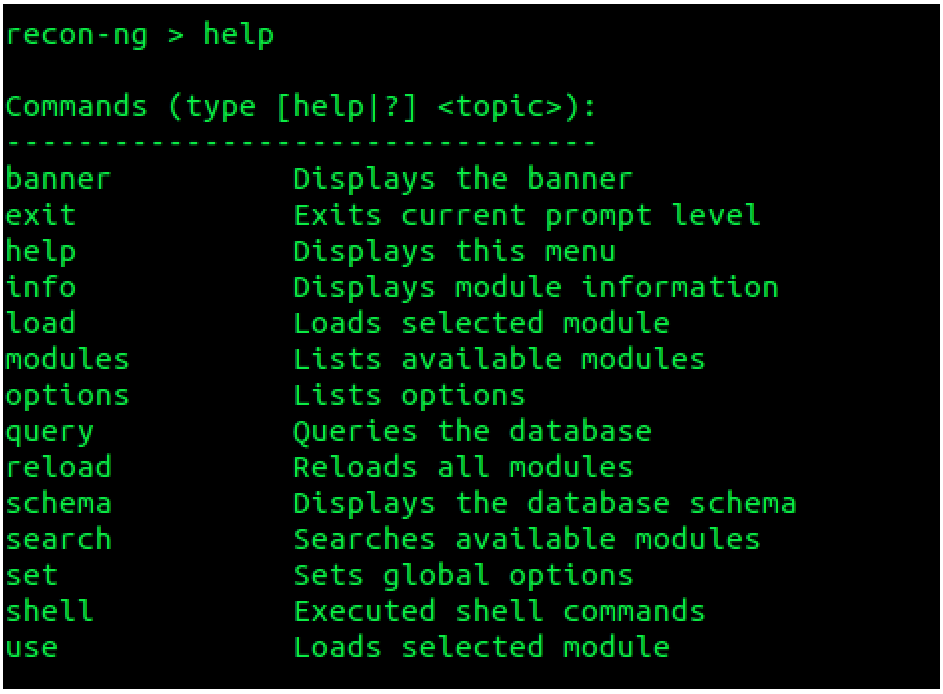
Discover Contacts And Domains With Recon-ng

pentestlab.blog/category/information-gathering/page/4

January 31, 2013

Automation is really important in penetration testing engagements because it can help the penetration tester to save time and to give more attention to other activities.For that reason many pen testers are putting effort to build tools to assist them with a variety of tasks.Such a tool is the recon-ng which can perform web-based reconnaissance and it can be used in social engineering engagements or for extracting information that exists on the web.In this article we will examine how we can use the Recon-Ng framework to discover different type of information.

We can type help in the framework in order to see a list with all the available commands.

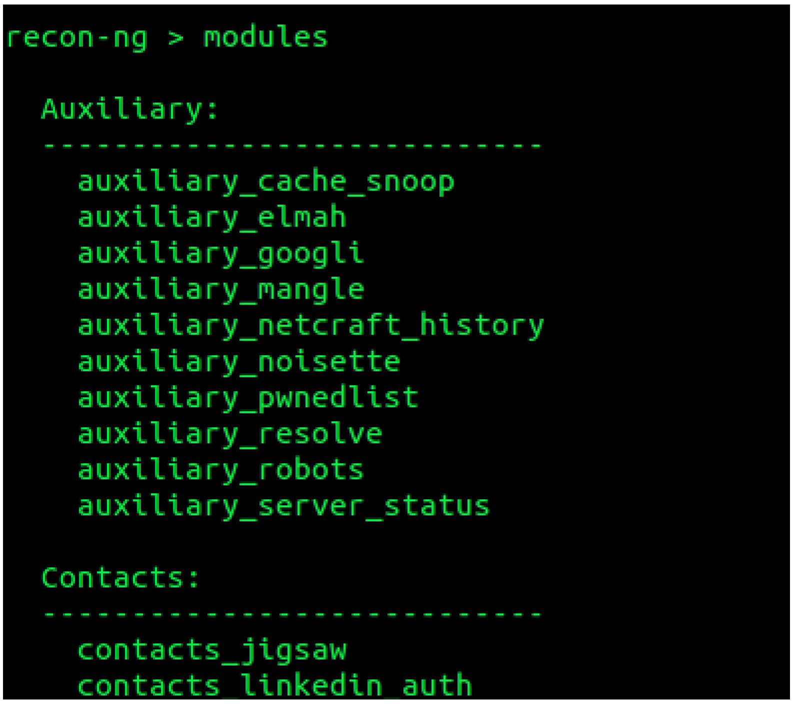


```
recon-ng > help

Commands (type [help|?] <topic>):
---------------------------------
banner          Displays the banner
exit            Exits current prompt level
help            Displays this menu
info            Displays module information
load            Loads selected module
modules         Lists available modules
options         Lists options
query           Queries the database
reload          Reloads all modules
schema          Displays the database schema
search          Searches available modules
set             Sets global options
shell           Executed shell commands
use             Loads selected module
```

recon-ng – commands

We can see that there is a command named modules.We will type that command to check the existing modules that we can use.In the next image you can see a sample of the available modules.



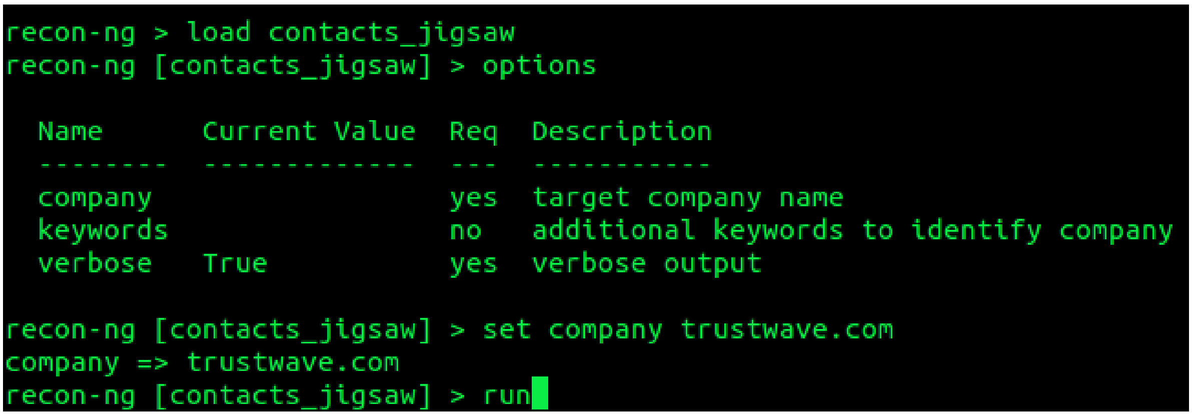
```
recon-ng > modules

  Auxiliary:
  ----------------------------
    auxiliary_cache_snoop
    auxiliary_elmah
    auxiliary_googli
    auxiliary_mangle
    auxiliary_netcraft_history
    auxiliary_noisette
    auxiliary_pwnedlist
    auxiliary_resolve
    auxiliary_robots
    auxiliary_server_status

  Contacts:
  ----------------------------
    contacts_jigsaw
    contacts_linkedin_auth
```

recon-ng – sample of the available modules

There is a module called contacts_jigsaw.Jigsaw is a website similar to Linkedin that contains a large database of business contacts.So let’s say that we want to discover the contacts of a company that exists on jigsaw.We will load the module with the command load contacts_jigsaw and we will set the domain of our preference.



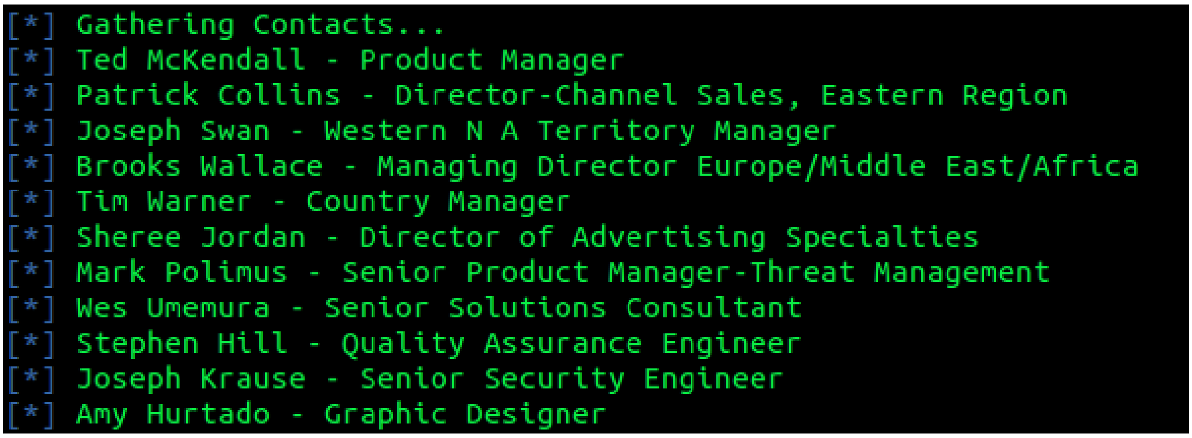
```
recon-ng > load contacts_jigsaw
recon-ng [contacts_jigsaw] > options

  Name      Current Value  Req  Description
  --------  -------------  ---  -----------
  company                  yes  target company name
  keywords                 no   additional keywords to identify company
  verbose   True           yes  verbose output

recon-ng [contacts_jigsaw] > set company trustwave.com
company => trustwave.com
recon-ng [contacts_jigsaw] > run
```

load jigsaw module

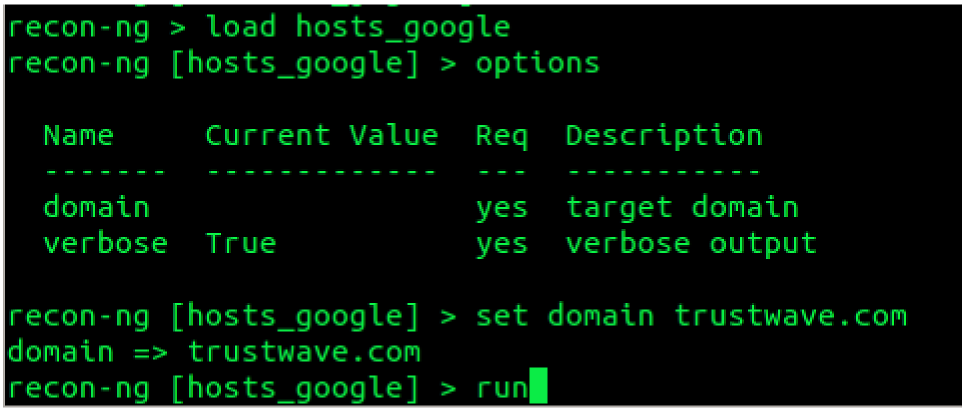
in the next image we can see a sample of the output:



```
[*] Gathering Contacts...
[*] Ted McKendall - Product Manager
[*] Patrick Collins - Director-Channel Sales, Eastern Region
[*] Joseph Swan - Western N A Territory Manager
[*] Brooks Wallace - Managing Director Europe/Middle East/Africa
[*] Tim Warner - Country Manager
[*] Sheree Jordan - Director of Advertising Specialties
[*] Mark Polimus - Senior Product Manager-Threat Management
[*] Wes Umemura - Senior Solutions Consultant
[*] Stephen Hill - Quality Assurance Engineer
[*] Joseph Krause - Senior Security Engineer
[*] Amy Hurtado - Graphic Designer
```

recon-ng – Gathering Contacts

Now that we have some contacts we can try to use the Google module to discover additional domains of the same company.



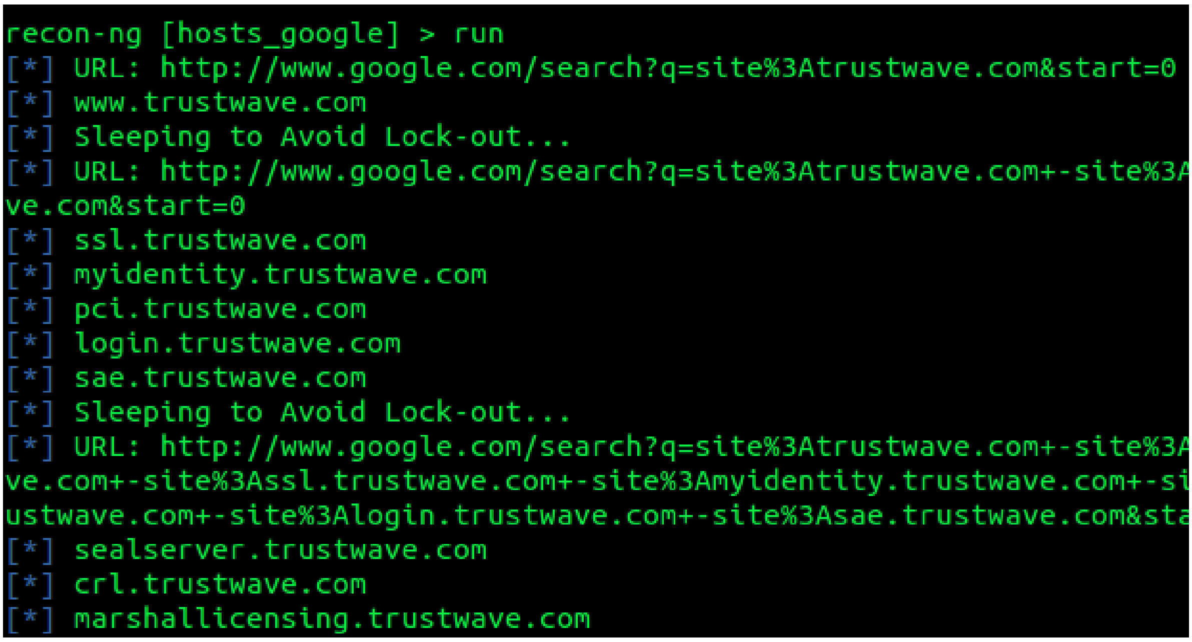
```
recon-ng > load hosts_google
recon-ng [hosts_google] > options

  Name     Current Value  Req  Description
  -------  -------------  ---  -----------
  domain                  yes  target domain
  verbose  True           yes  verbose output

recon-ng [hosts_google] > set domain trustwave.com
domain => trustwave.com
recon-ng [hosts_google] > run
```

discover hosts via google

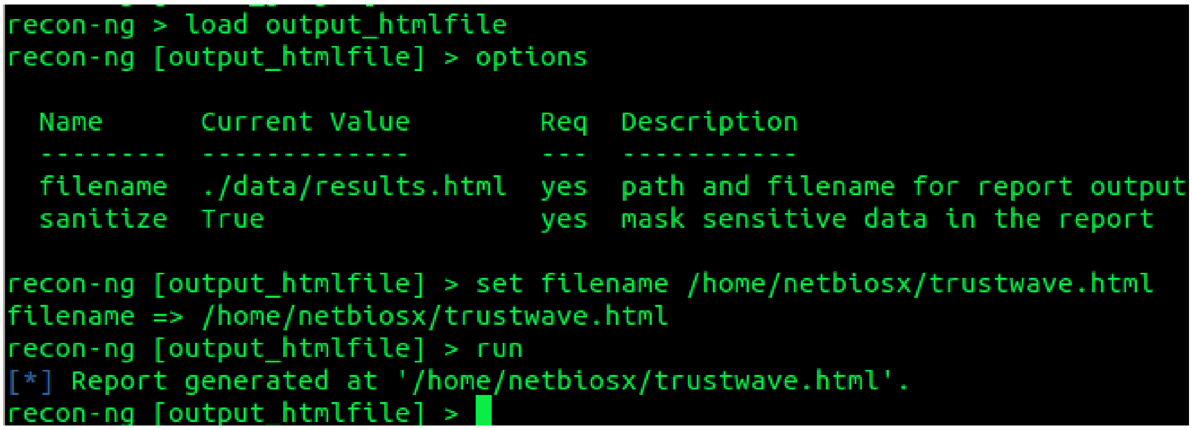
In the image below we can see a sample of the results that recon-ng has produced.



```
recon-ng [hosts_google] > run
[*] URL: http://www.google.com/search?q=site%3Atrustwave.com&start=0
[*] www.trustwave.com
[*] Sleeping to Avoid Lock-out...
[*] URL: http://www.google.com/search?q=site%3Atrustwave.com+-site%3A
ve.com&start=0
[*] ssl.trustwave.com
[*] myidentity.trustwave.com
[*] pci.trustwave.com
[*] login.trustwave.com
[*] sae.trustwave.com
[*] Sleeping to Avoid Lock-out...
[*] URL: http://www.google.com/search?q=site%3Atrustwave.com+-site%3A
ve.com+-site%3Assl.trustwave.com+-site%3Amyidentity.trustwave.com+-si
ustwave.com+-site%3Alogin.trustwave.com+-site%3Asae.trustwave.com&sta
[*] sealserver.trustwave.com
[*] crl.trustwave.com
[*] marshallicensing.trustwave.com
```

Discovering subdomains with recon-ng

Recon-ng gives us also the ability to extract the results in CSV format or in an HTML file.



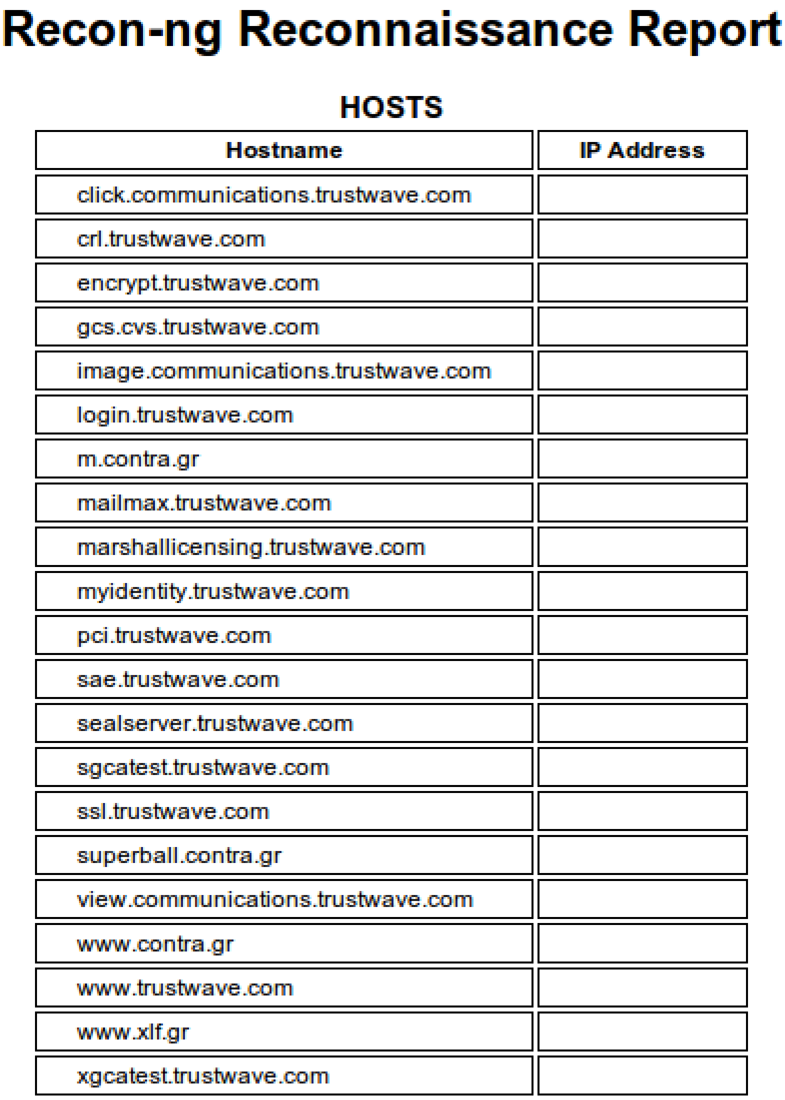
```
recon-ng > load output_htmlfile
recon-ng [output_htmlfile] > options

  Name      Current Value        Req  Description
  --------  -------------        ---  -----------
  filename  ./data/results.html  yes  path and filename for report output
  sanitize  True                 yes  mask sensitive data in the report

recon-ng [output_htmlfile] > set filename /home/netbiosx/trustwave.html
filename => /home/netbiosx/trustwave.html
recon-ng [output_htmlfile] > run
[*] Report generated at '/home/netbiosx/trustwave.html'.
recon-ng [output_htmlfile] >
```

Save the results in HTML file

You can see in the next two images the output of the report:

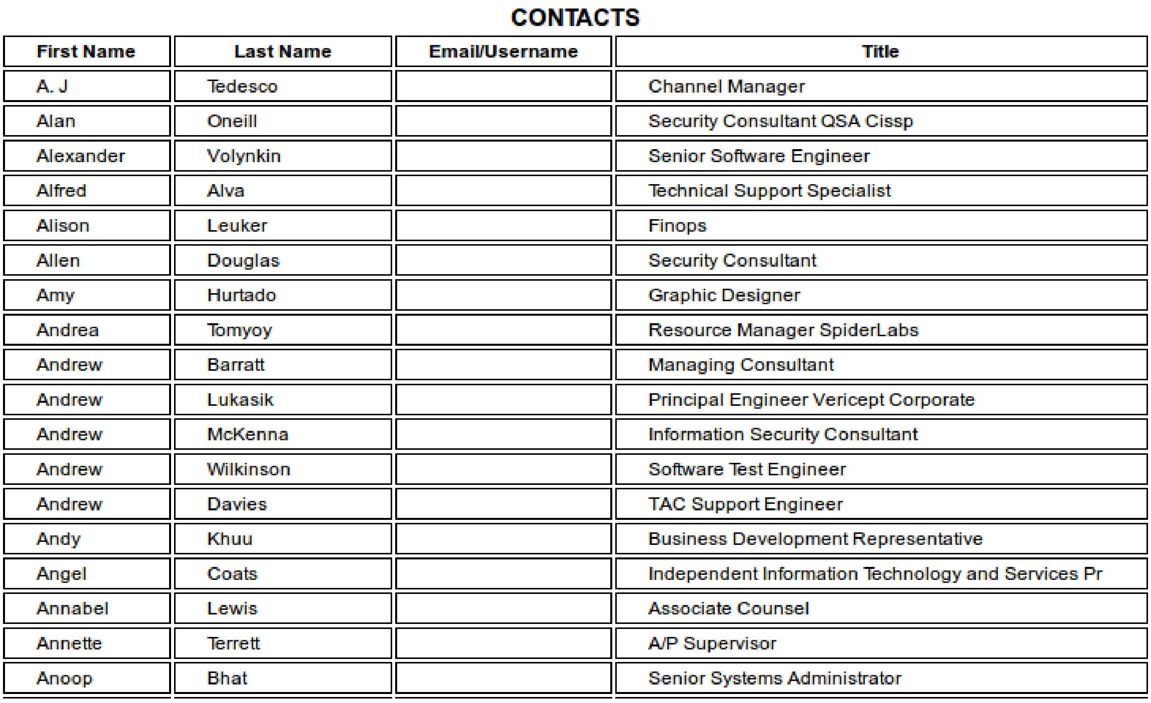


Recon-ng Reconnaissance Report

HOSTS

Hostname	IP Address
click.communications.trustwave.com	
crl.trustwave.com	
encrypt.trustwave.com	
gcs.cvs.trustwave.com	
image.communications.trustwave.com	
login.trustwave.com	
m.contra.gr	
mailmax.trustwave.com	
marshallicensing.trustwave.com	
myidentity.trustwave.com	
pci.trustwave.com	
sae.trustwave.com	
sealserver.trustwave.com	
sgcatest.trustwave.com	
ssl.trustwave.com	
superball.contra.gr	
view.communications.trustwave.com	
www.contra.gr	
www.trustwave.com	
www.xlf.gr	
xgcatest.trustwave.com	

recon-ng – Report



CONTACTS

First Name	Last Name	Email/Username	Title
A. J	Tedesco		Channel Manager
Alan	Oneill		Security Consultant QSA Cissp
Alexander	Volynkin		Senior Software Engineer
Alfred	Alva		Technical Support Specialist
Alison	Leuker		Finops
Allen	Douglas		Security Consultant
Amy	Hurtado		Graphic Designer
Andrea	Tomyoy		Resource Manager SpiderLabs
Andrew	Barratt		Managing Consultant
Andrew	Lukasik		Principal Engineer Vericept Corporate
Andrew	McKenna		Information Security Consultant
Andrew	Wilkinson		Software Test Engineer
Andrew	Davies		TAC Support Engineer
Andy	Khuu		Business Development Representative
Angel	Coats		Independent Information Technology and Services Pr
Annabel	Lewis		Associate Counsel
Annette	Terrett		A/P Supervisor
Anoop	Bhat		Senior Systems Administrator

recon-ng report contacts

Conclusion

Recon-ng is a great framework that can help in the information gathering stage of a penetration test.This tool is really simple to use and it holds every result in its database for later use.The report that generates is well formatted and if in the future additional modules will added on the framework then it will included in every penetration tester toolkit.