Certified Ethical Hacking With Penetration Testing

CEHWPT

LABS Course

LAB3 working with Reconnaissance tools

Prepared by Eng. Khaled Gamo

15-6-2019

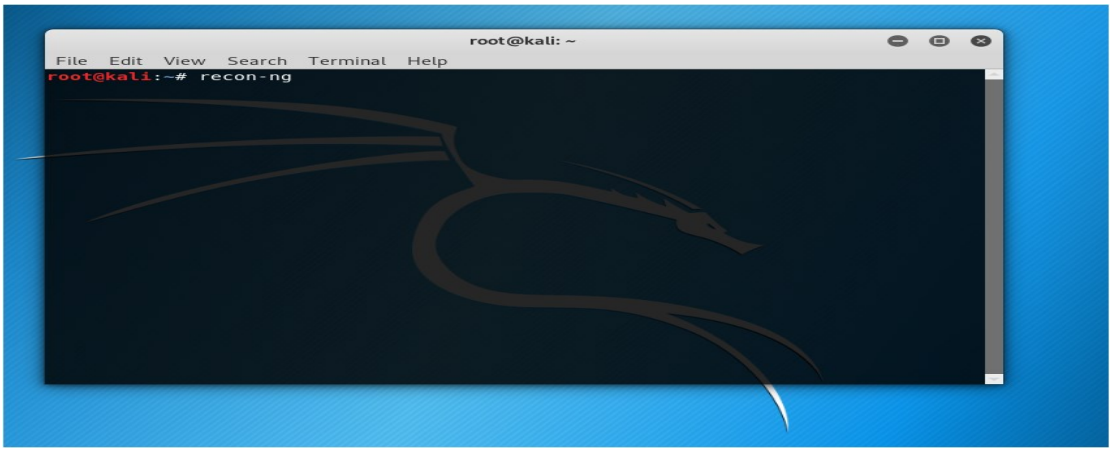
LAB3 working with Reconnaissance tools

Working with recon-ng

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 lab we will examine how we can use the Recon-Ng framework to discover different type of information.

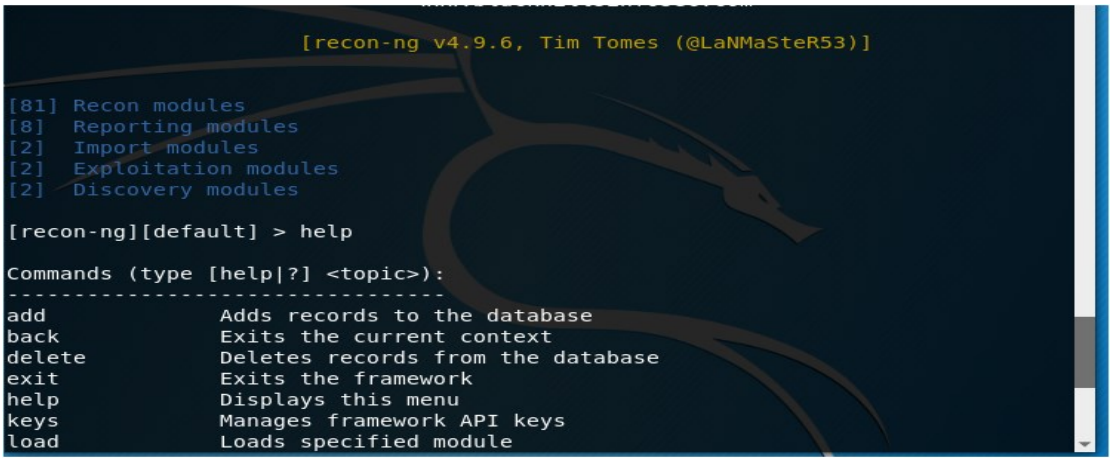
Step 1: Starting Recon-ng

In kali terminal use the command recon-ng and press enter



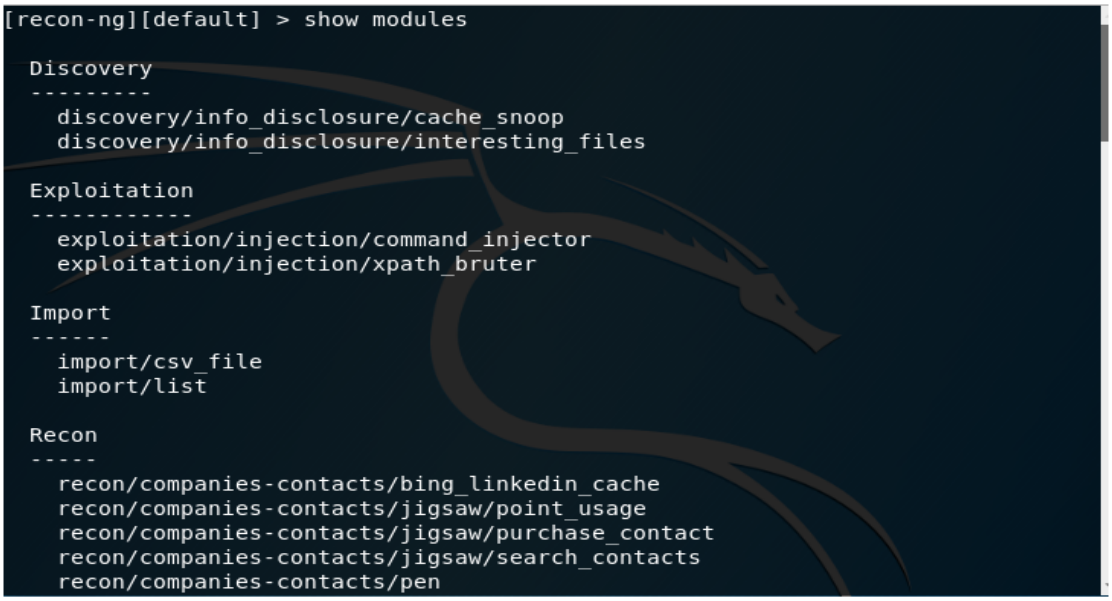
Step 2: Viewing Commands

At the prompt, let's type help in order to look at the commands we can use in Recon-ng.recon-ng > help



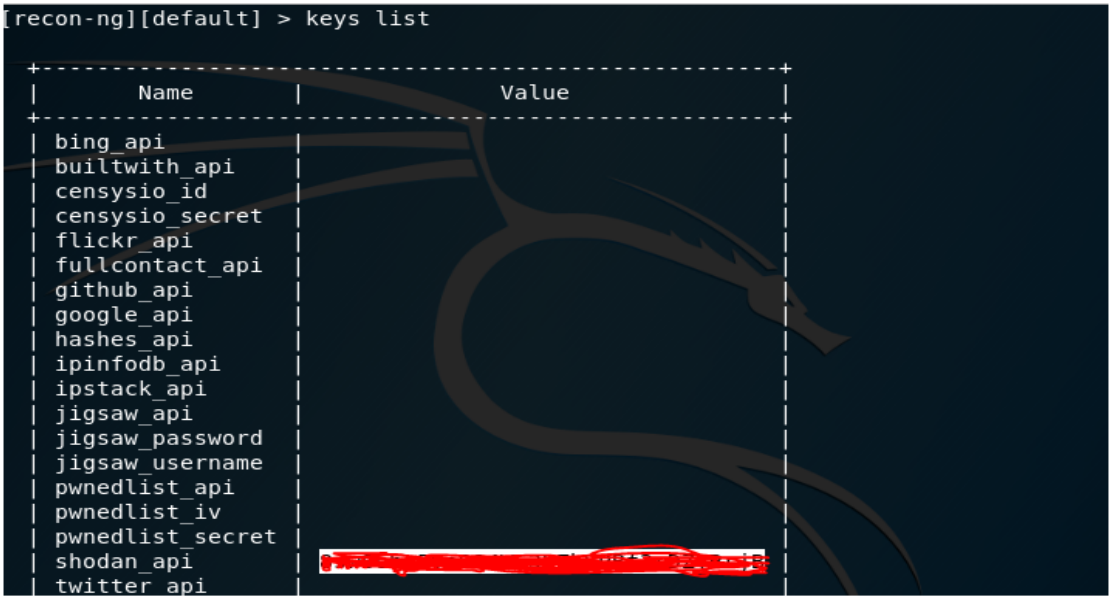
Step 3: Showing Modules

To see all the modules in Recon-ng, we can type: **recon-ng > show modules**

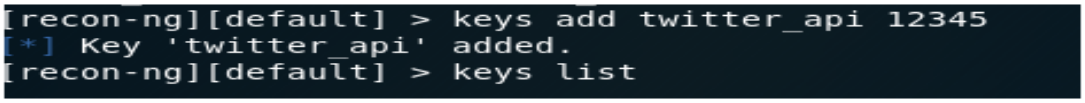


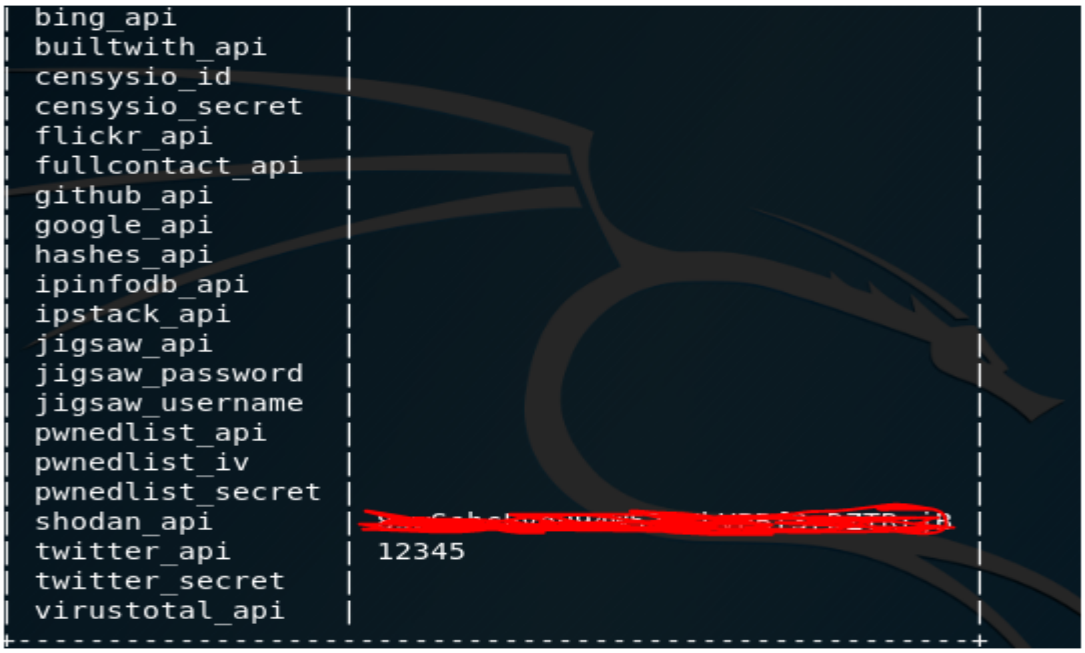
Step 4: Viewing Keys

One of the strengths and beauties of Recon-ng is the use of various application programming interfaces (APIs) to extract useful recon information. For instance, Recon-ng can use Bing, Google, Facebook, Instagram, LinkedIn, and other online applications once you get the API key. With that key, you have almost unlimited access to that application. To see what API keys Recon-ng can use, type: **recon-ng > keys list**



When you obtain an API key and you want to add it to Recon-ng for use, you simply add it to the keys. For instance, if I received an API key from twitter and that key was "12345", I could add it to Recon -ng by typing: recon-ng > keys add twitter_api 12345 Now when you list the keys, you can see that your twitter_api key is listed. This means that when you use the twitter recon module, it will automatically use this key to access twitter like a twitter application would





Step 5: create a workspace

We need to know is that things can get messy dealing with hosts, domain names and contacts etc. when you make intelligence gathering. In order to make things clear, there is a workspace concept. You can create, delete and see workspaces. By default, there is supposed to be [recon-ng][default] in your command line. When you type 'workspaces' and hit the enter, you see the commands with workspace. You can create a new one with add selection like 'workspaces add newworkspace'. As you'd probably guess, you should jump into workspaces by selecting them like 'workspaces select newworkspace'.

```
[recon-ng][default] > workspaces
Manages workspaces

Usage: workspaces [list|add|select|delete]

[recon-ng][default] > workspaces add newworkspace
```

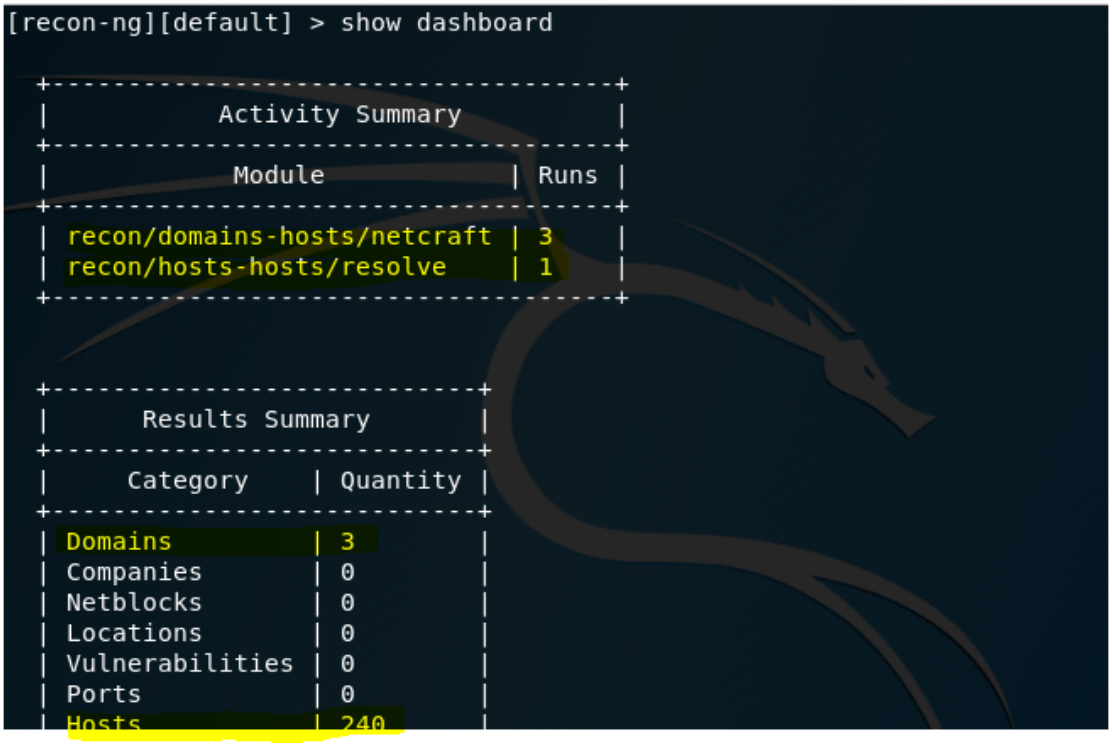
Step 6: Viewing Schema

There are several of inputs we can add, delete or change like domains, company name, contacts, profiles etc. Those normally change based on the workspace you work on. You can manage all of them typing 'show schema'. Most of inputs are directly connected to each other.

```
recon-ng][newworkspace] > show schema
 +-----------------+
 |     domains     |
 +-----------------+
 | domain | TEXT |
 | module | TEXT |
 +-----------------+

 +---------------------+
 |      companies      |
 +---------------------+
 | company     | TEXT  |
 | description | TEXT  |
 | module      | TEXT  |
 +---------------------+

 +-------------------+
 |     netblocks     |
 +-------------------+
 | netblock | TEXT   |
 | module   | TEXT   |
 +-------------------+

 +-------------------------+
 |        locations        |
 +-------------------------+
 | latitude       | TEXT   |
 | longitude      | TEXT   |
 | street_address | TEXT   |
 | module         | TEXT   |
 +-------------------------+
```

Step 7: Viewing Dashboard

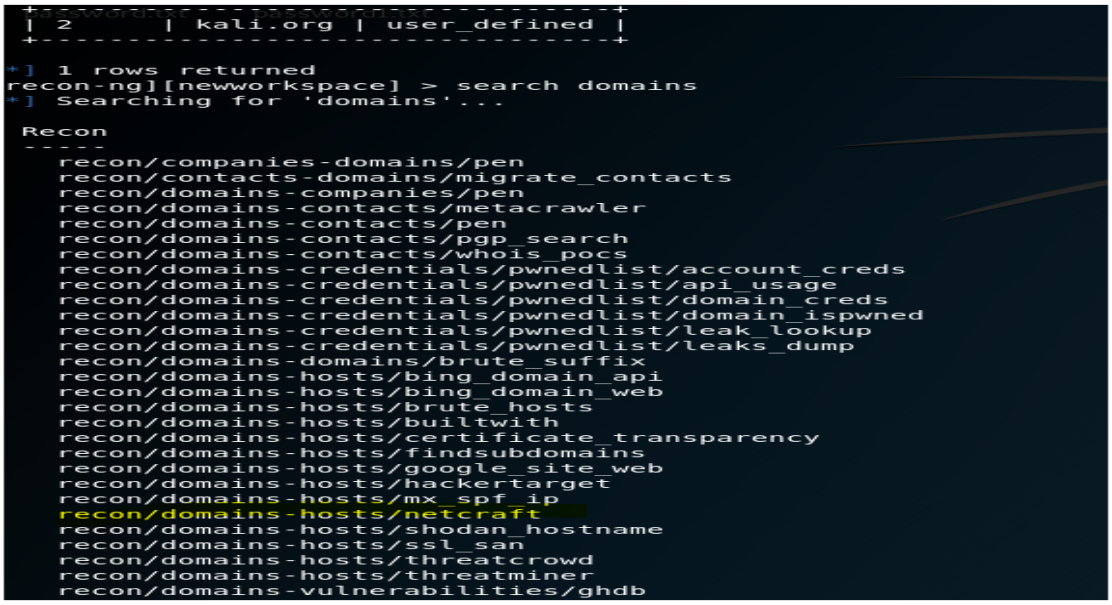
By using command show dashboard we can have a look at the current content of the database note in our example we return to default workspace and show the database of default workspace since all activity was in default workspace.



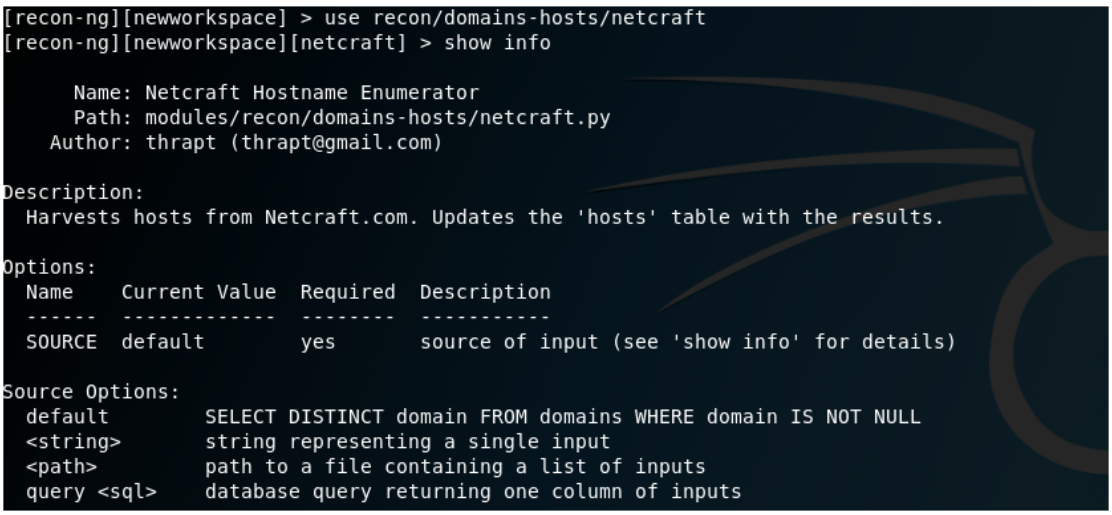
How to retrieve subdomains, ip, region, country and location for a particular domain?

Aim: To get domain corresponding subdomains, ip, region, country and location.
Procedure:

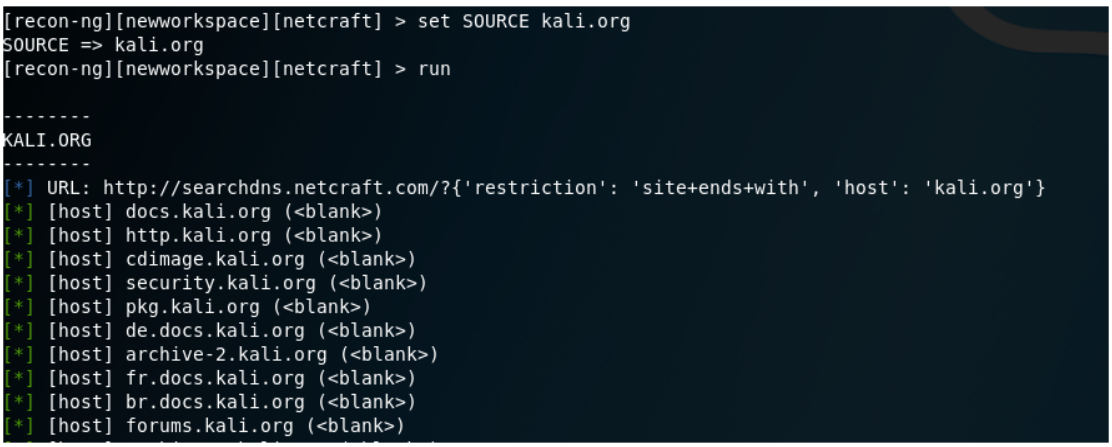
Step1: For finding the subdomains use netcraft module " use recon/domains-hosts/netcraft". You can find the module using show modules or search domains



Step2: Use command show info to find the requirements of the module.



Step3: Set the source kali.org and run the module



We found 37 hosts belong to kali.org

```
[*] [host] archive-10.kali.org (<blank>)
[*] [host] id.docs.kali.org (<blank>)
[*] [host] old.kali.org (<blank>)
[*] [host] archive-11.kali.org (<blank>)
[*] [host] cn.docs.kali.org (<blank>)
[*] [host] images.kali.org (<blank>)
[*] [host] archive-9.kali.org (<blank>)
[*] [host] archive-8.kali.org (<blank>)
[*] [host] bugs.kali.org (<blank>)
[*] [host] repo.kali.org (<blank>)
[*] [host] archive-5.kali.org (<blank>)
[*] [host] nl.docs.kali.org (<blank>)
[*] [host] ru.docs.kali.org (<blank>)
[*] [host] archive.kali.org (<blank>)
[*] [host] archive-12.kali.org (<blank>)
[*] [host] ja.docs.kali.org (<blank>)

-------
SUMMARY
-------
[*] 37 total (37 new) hosts found.
```

Step3: For finding the ipaddress use the resolve module " use recon/hosts-hosts/resolve".

```
[recon-ng][newworkspace] > use recon/hosts-hosts/resolve
[recon-ng][newworkspace][resolve] > run
[*] docs.kali.org => 192.124.249.10
[*] http.kali.org => 192.99.200.113
[*] cdimage.kali.org => 192.99.200.113
[*] security.kali.org => 192.99.200.113
[*] pkg.kali.org => 192.124.249.9
[*] de.docs.kali.org => 192.124.249.10
[*] archive-2.kali.org => 192.99.150.27
[*] fr.docs.kali.org => 192.124.249.10
[*] br.docs.kali.org => 192.124.249.10
[*] forums.kali.org => 192.124.249.12
[*] archive-4.kali.org => 149.202.201.51
[*] ar.docs.kali.org => 192.124.249.10
[*] archive-7.kali.org => 209.126.116.149
[*] git.kali.org => 67.23.72.103
[*] downloads.kali.org => 149.56.27.8
[*] downloads.kali.org => 192.99.63.209
[*] downloads.kali.org => 23.237.148.130
[*] downloads.kali.org => 199.189.86.7
[*] downloads.kali.org => 188.138.17.16
[*] es.docs.kali.org => 192.124.249.10
[*] tools.kali.org => 192.124.249.6
[*] it.docs.kali.org => 192.124.249.10
```

```
[*] archive-8.kali.org => 192.99.200.113
[*] bugs.kali.org => 192.124.249.169
[*] repo.kali.org => 144.217.77.182
[*] archive-5.kali.org => 192.99.150.28
[*] nl.docs.kali.org => 192.124.249.10
[*] ru.docs.kali.org => 192.124.249.10
[*] archive.kali.org => 192.99.45.140
[*] archive-12.kali.org => 167.114.101.174
[*] ja.docs.kali.org => 192.124.249.10

-------
SUMMARY
-------
[*] 8 total (8 new) hosts found.
```

How to get contacts and email id's of particular domain?

Aim: To get contacts and email id's of a domain.

Procedure:

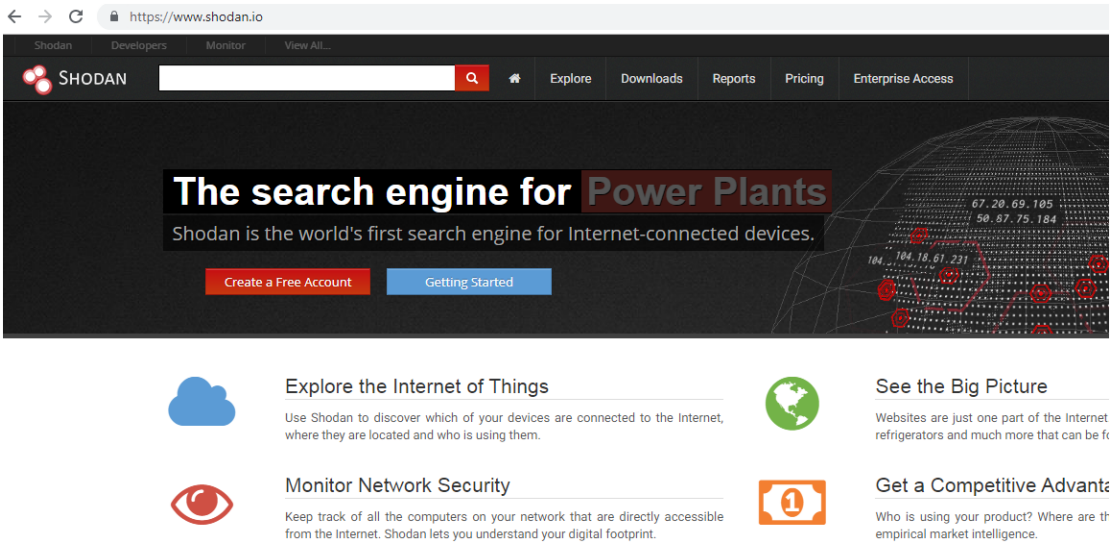
Step1: For retrieving the contacts we need to use the pgp_search module "use recon/domains-contacts/pgp_search".

Step2: Use command show options for finding the requirements of the module.

Step3: Give the command show contacts so we will retrieve a table which contains the contact information along with the emailed.

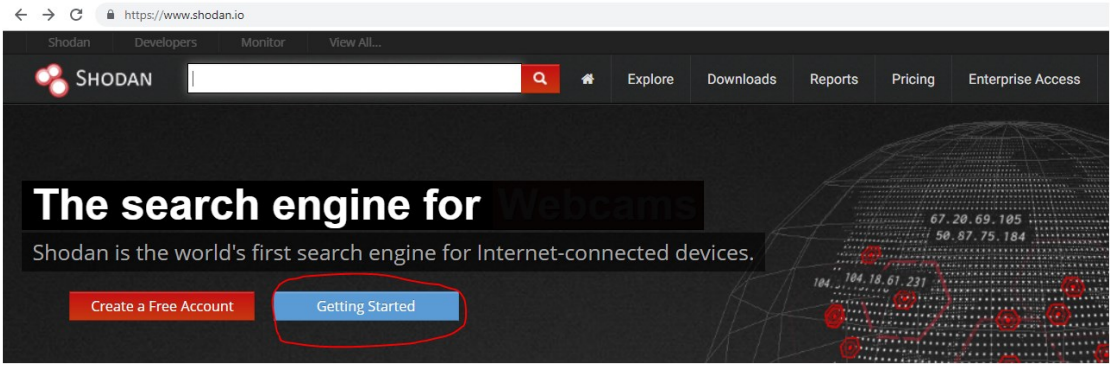
Working with Shodan

Step1: browsing https://www.shodan.io/

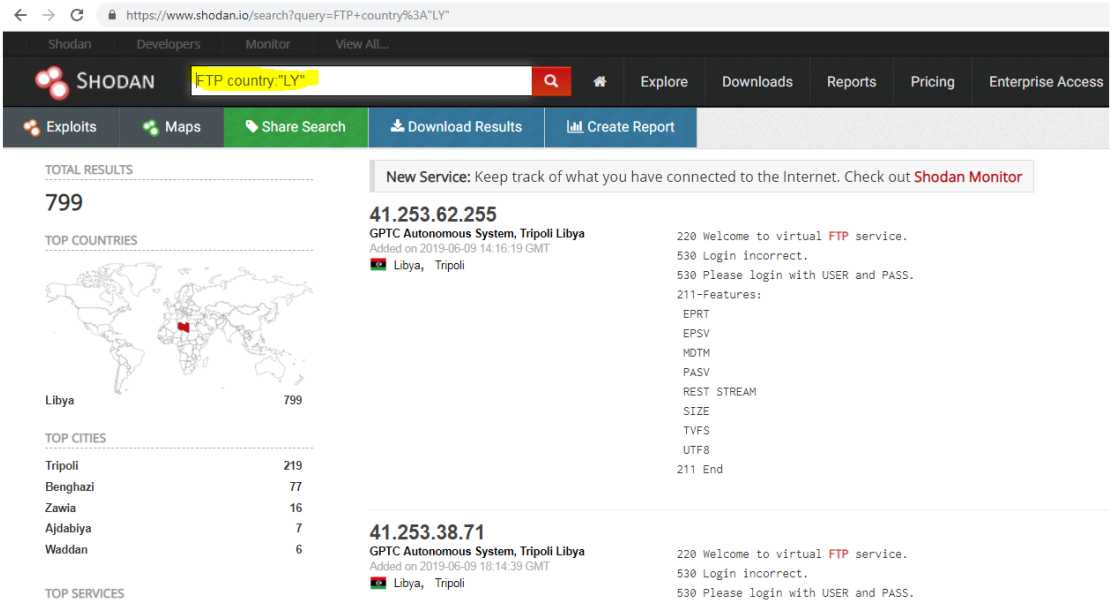


- Basic Operations: Login
- Login using one of several other options (Google, Twitter, Yahoo, AOL, Facebook, OpenID
- Login is not required, but country and net filters are not available unless you login.
- Export requires you to be logged in.

Step 2: press Getting Started

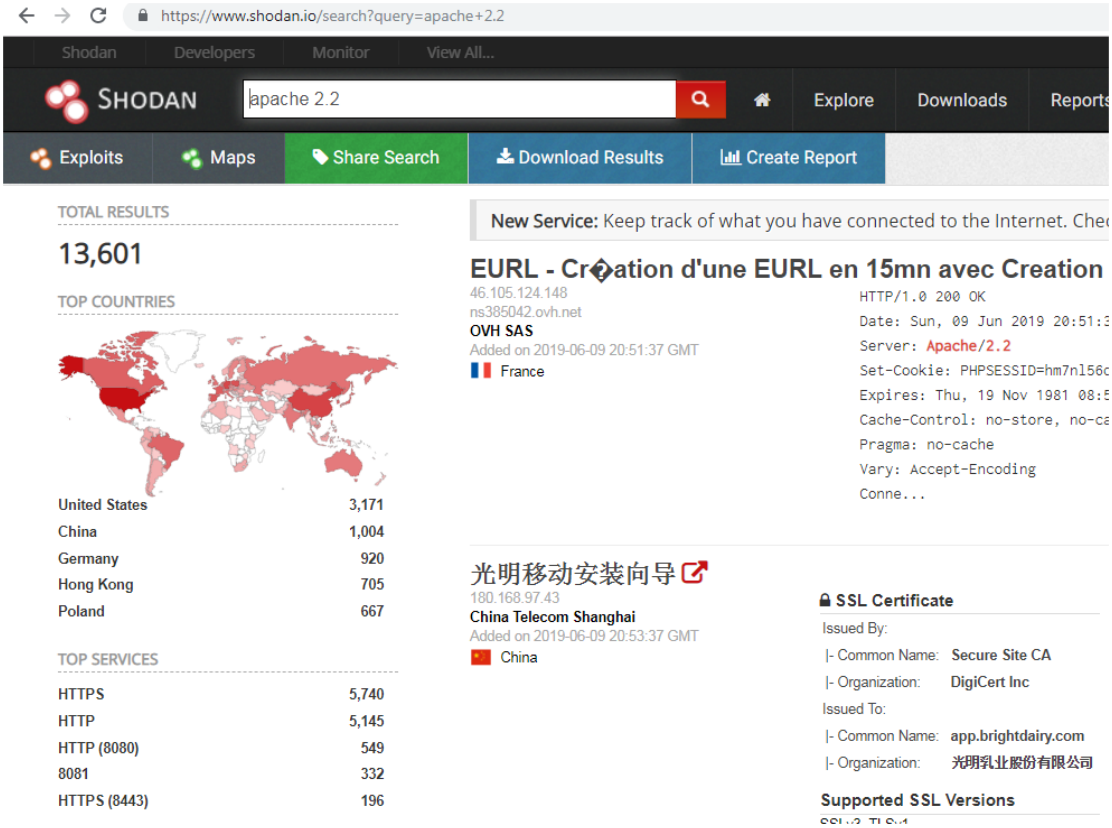


Step 3: exploring Shodan for example we looking for FTP server in Libya we will use filter FTP country: "LY" we found 799 FTP servers



Step 3: looking for Apache/2.2

We found 13,601 apache 2.2 all over the world top country USA, China, Germany



Using Shodan for penetration Testing

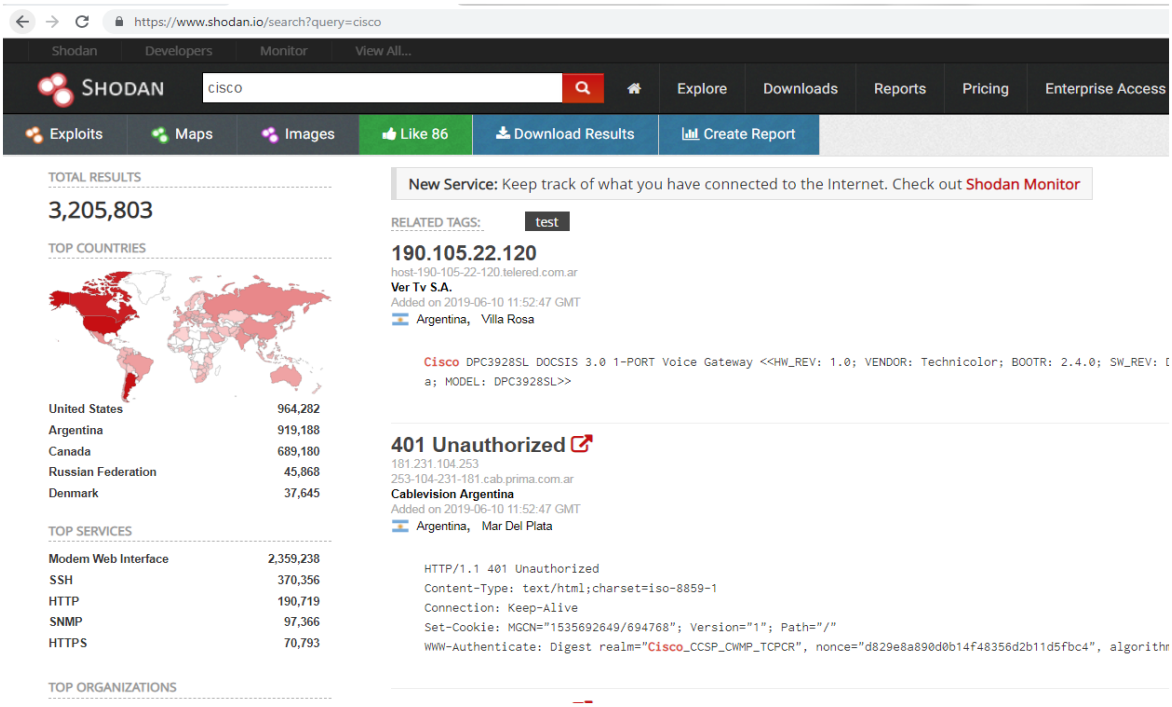
- Using SHODAN for penetration testing requires some basic knowledge of banners including HTTP status codes**.**
- Banners advertise service and version

HTTP Status Codes

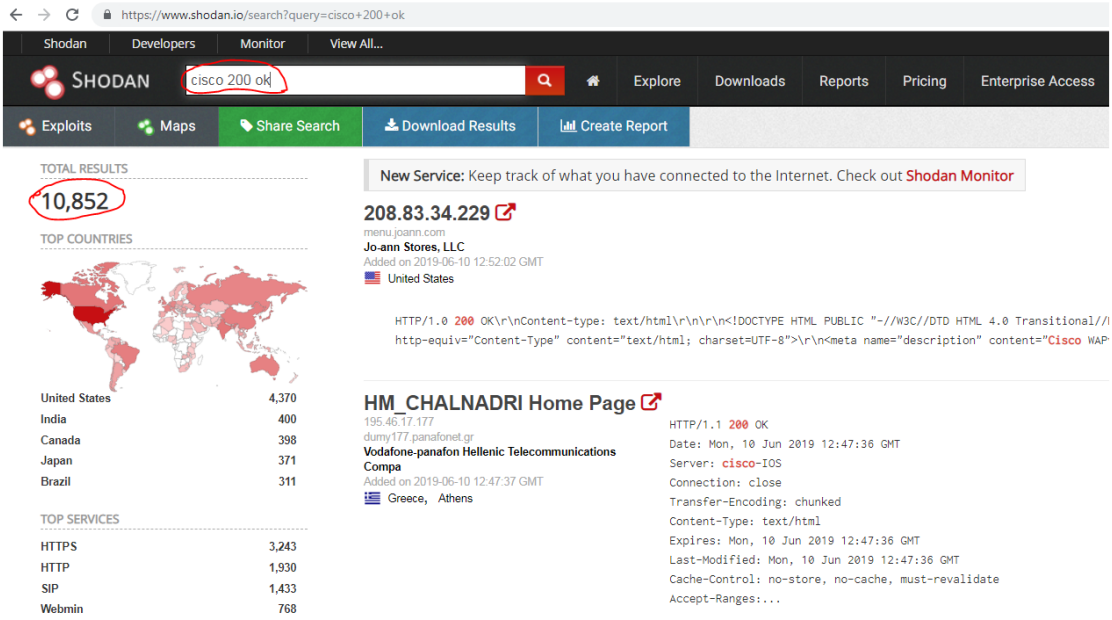
Status Code	Description
200 OK	Request succeeded
401 Unauthorized	Request requires authentication
403 Forbidden	Request is denied regardless of authentication

Case Study: Cisco Devices

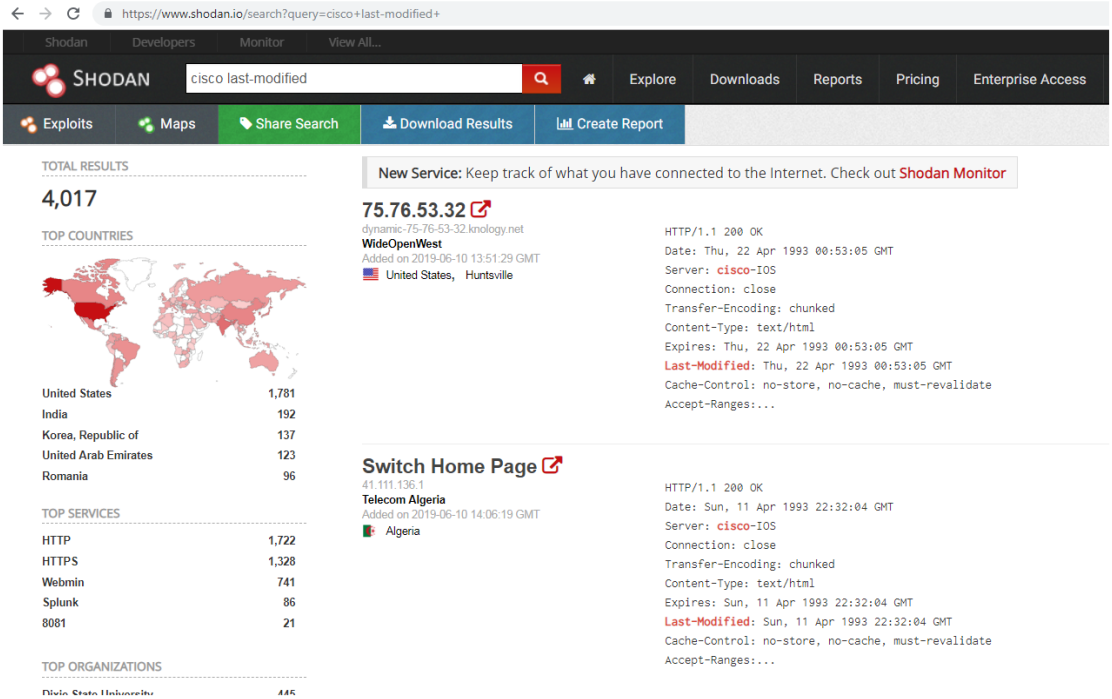
Step1: In shodan search write cisco and press enter



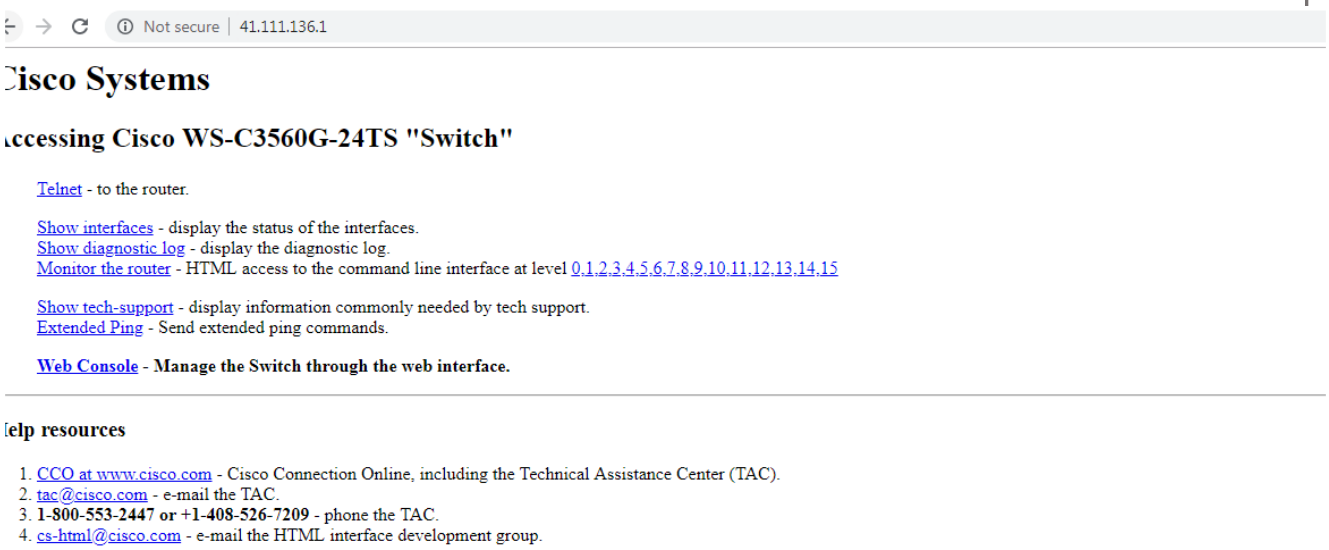
Step2: let us try using filter cisco 200 ok

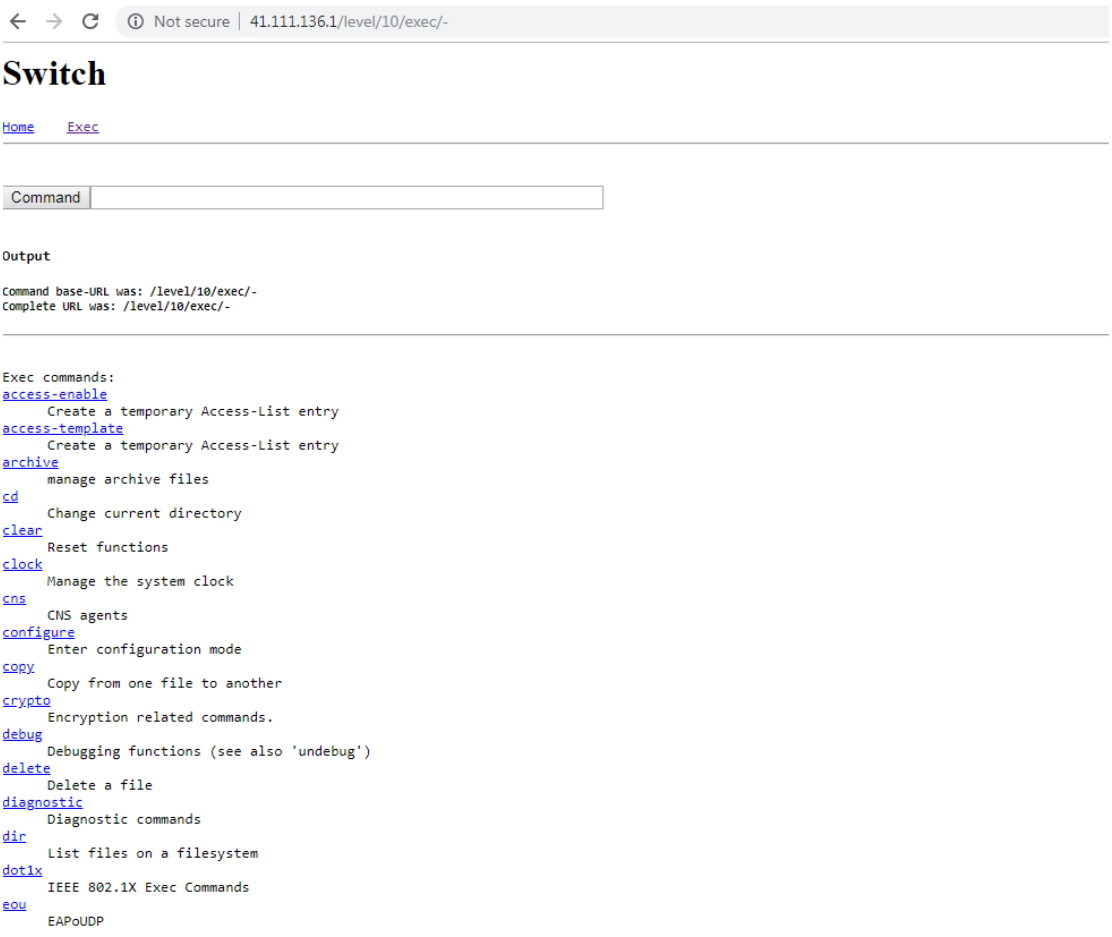


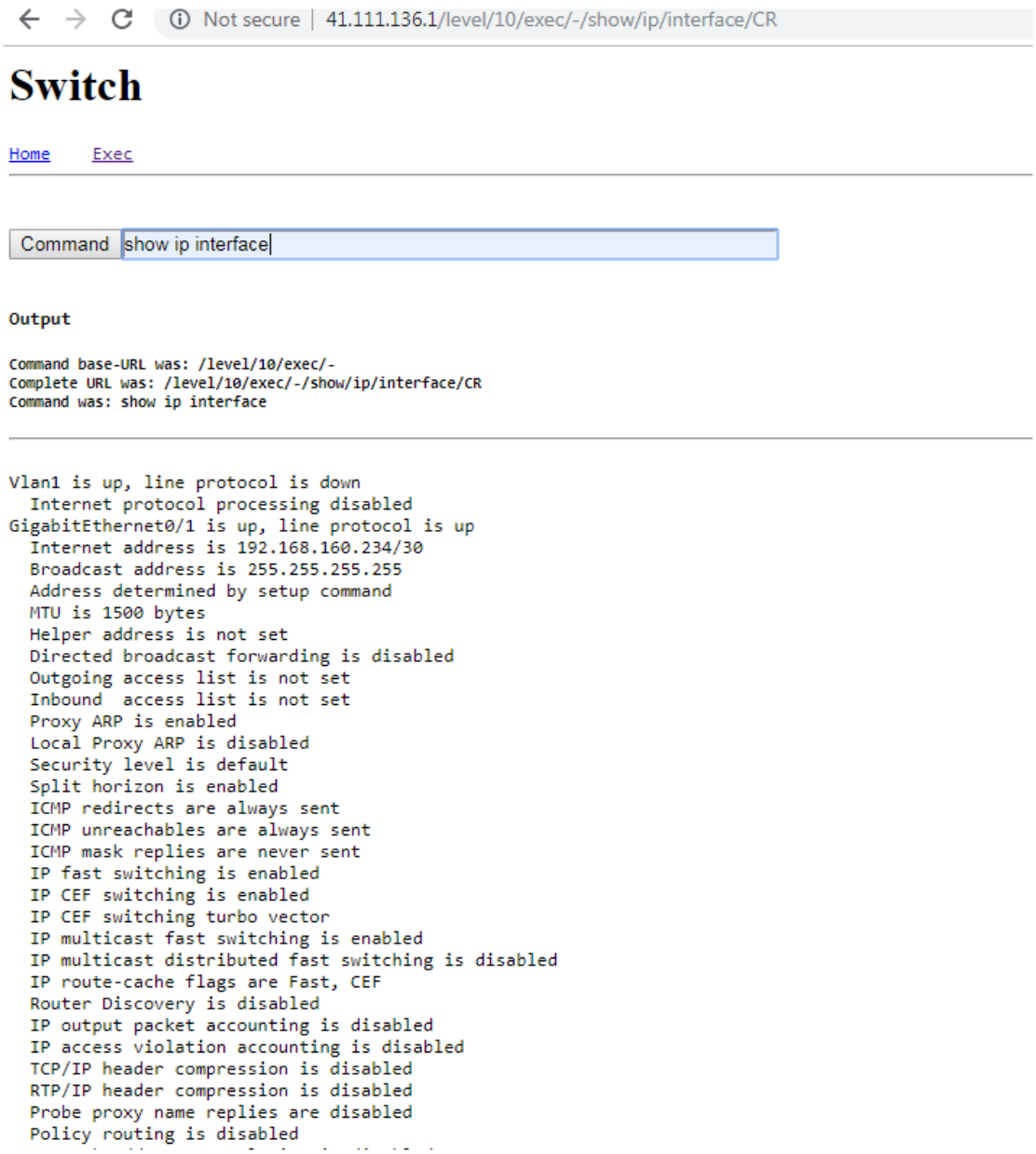
Step3: let us try cisco last modified



We can found many cisco device without authentication in the internet using shodan such as




Not secure | 41.111.136.1/level/10/exec/-
Switch
Home Exec
Command
Output
Command base-URL was: /level/10/exec/-
Complete URL was: /level/10/exec/-
Exec commands:
access-enable
Create a temporary Access-List entry
access-template
Create a temporary Access-List entry
archive
manage archive files
cd
Change current directory
clear
Reset functions
clock
Manage the system clock
cns
CNS agents
configure
Enter configuration mode
copy
Copy from one file to another
crypto
Encryption related commands.
debug
Debugging functions (see also 'undebug')
delete
Delete a file
diagnostic
Diagnostic commands
dir
List files on a filesystem
dot1x
IEEE 802.1X Exec Commands
eou
EAPoUDP


Not secure | 41.111.136.1/level/10/exec/-/show/ip/interface/CR
Switch
Home Exec
Command show ip interface
Output
Command base-URL was: /level/10/exec/-
Complete URL was: /level/10/exec/-/show/ip/interface/CR
Command was: show ip interface
Vlan1 is up, line protocol is down
Internet protocol processing disabled
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.160.234/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled

Working with the harvester Tools

The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.

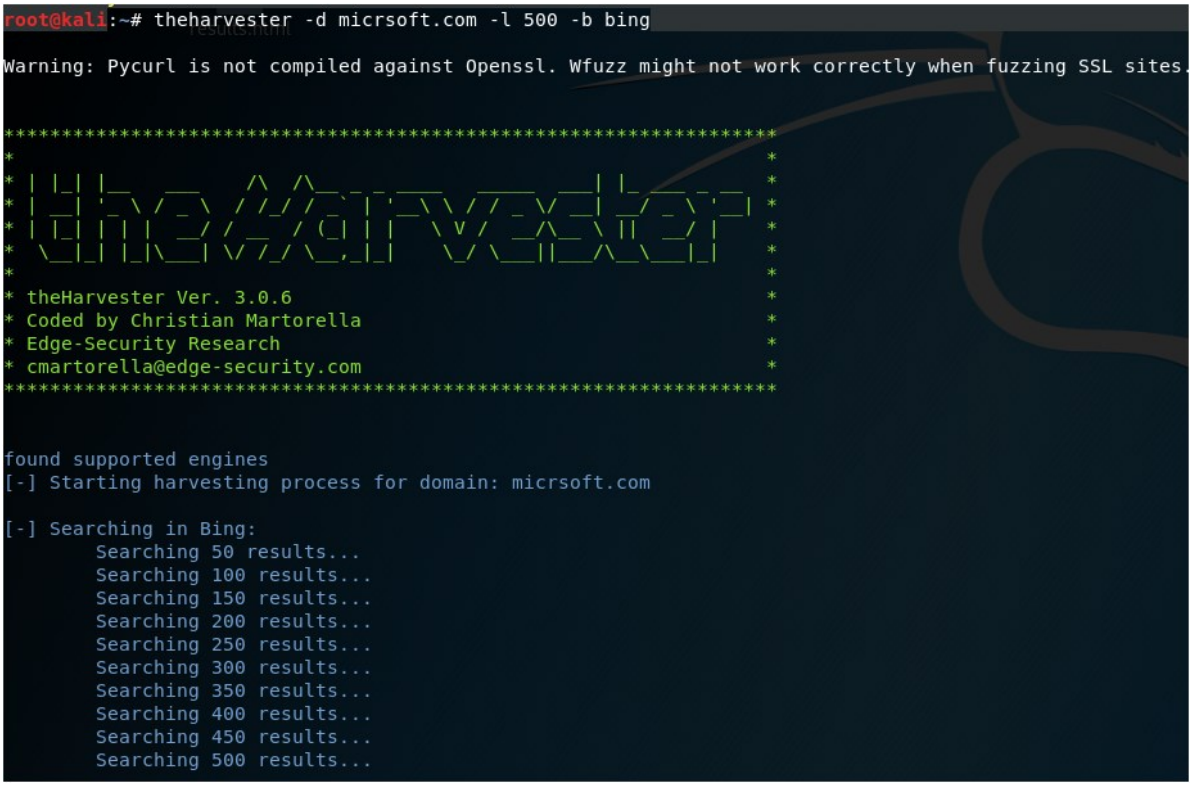
This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization.

This is a complete rewrite of the tool with new features like:

- Time delays between request
- All sources search
- Virtual host verifier
- Active enumeration (DNS enumeration, Reverse lookups, TLD expansion)
- Integration with SHODAN computer database, to get the open ports and banners
- Save to XML and HTML
- Basic graph with stats
- New sources

Step1: starting the tools we can use command theharvester in kali terminal.

Step2: using the command theharvester –d Microsoft.com –l 500 –b bing



```
Harvesting results
No IP addresses found


[+] Emails found:
------------------
hcjang@micrsoft.com
dotnetnative@micrsoft.com
'billgates@micrsoft.com
edwardgates@micrsoft.com
leans@micrsoft.com
tell_fs@micrsoft.com
a-sr...@micrsoft.com
xxxxxxx@micrsoft.com
MsftConn@micrsoft.com
jsmith@micrsoft.com
bns@micrsoft.com
Research,dechakr@micrsoft.com
some...@micrsoft.com
winpx@micrsoft.com
inclusivedesign@micrsoft.com
5kentoy@micrsoft.com
mavern@micrsoft.com
prcfd@micrsoft.com
b-adrijs@micrsoft.com
j-jorgep@micrsoft.com
ammons@micrsoft.com
someone@micrsoft.com
a-savk@micrsoft.com
Vishal.Joshi@micrsoft.com
tonyone23@micrsoft.com
snipped-for-privacy@micrsoft.com
inet@micrsoft.com
t...@micrsoft.com
tfwst@micrsoft.com
a-bswan@micrsoft.com
jiawgu@micrsoft.com
gray@micrsoft.com
```

Step3: using the command theharvester –d Microsoft.com –l 500 –b google

```
root@kali:~# theharvester -d micrsoft.com -l 500 -b google

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.


*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester Ver. 3.0.6                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


found supported engines
[-] Starting harvesting process for domain: micrsoft.com

[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...
        Searching 400 results...
        Searching 500 results...

Harvesting results
No IP addresses found
```

```
[+] Emails found:
------------------
gates@micrsoft.com
msnhst@micrsoft.com
account-security-noraply@micrsoft.com
josegonzalez@micrsoft.com
rlawrence@micrsoft.com
mcphelp@micrsoft.com
inclusivedesign@micrsoft.com
zdeng@online.micrsoft.com
v-siwils@micrsoft.com
houwen.peng@micrsoft.com
leans@micrsoft.com
dinei@micrsoft.com
scottr@micrsoft.com
edwardgates@micrsoft.com
morons@micrsoft.com
quarantine@messaging.micrsoft.com

[+] Hosts found in search engines:
-----------------------------------

Total hosts: 24

[-] Resolving hostnames IPs...

Account.micrsoft.com:empty
XXX.micrsoft.com:empty
account.micrsoft.com:empty
connect.micrsoft.com:empty
demos.micrsoft.com:empty
docs.micrsoft.com:empty
fareast.corp.micrsoft.com:empty
go.micrsoft.com:empty
login.micrsoft.com:empty
messaging.micrsoft.com:empty
msdn.micrsoft.com:empty
office.micrsoft.com:empty
online.micrsoft.com:empty
```

Step4: using the command theharvester –d Microsoft.com –l 500 –b linkedin