Certified Ethical Hacking With Penetration Testing CEHWPT

LABS Course

LAB3 working with Reconnaissance tools

Prepared by Eng. Khaled Gamo

17-1-2021

Recon-ng v5

In this recon-ng v5 tutorial, you will discover open source intelligence and easily pivot to new results. Find targets and move to discovering vulnerabilities.

What is recon-ng?

Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience

Running recon-ng from the command line, you enter a shell like environment where you can configure options, perform recon and output results to different report types.

The interactive console provides a number of helpful features such as command completion and contextual help.

Recon-ng 5 comes without modules, which is also one of the major differences. In addition, the parameters, commands, etc. have changed a bit to the previous versions.

Let us start our LAB

1- Starting recon ng using recon-ng command

2- Check available command using?

```
[recon-ng][default] > ?

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces
```

3- Options list command will displays the current settings and with options set the parameters (e.g. Name Server, Proxy, User-Agent) can be changed

```
[recon-ng][default] > options list

  Name        Current Value  Required  Description
  ----------  -------------  --------  -----------
  NAMESERVER  8.8.8.8        yes       default nameserver for the resolver m
xin
  PROXY                      no        proxy server (address:port)
  THREADS     10             yes       number of threads (where applicable)
  TIMEOUT     10             yes       socket timeout (seconds)
  USER-AGENT  Recon-ng/v5    yes       user-agent string
  VERBOSITY   1              yes       verbosity level (0 = minimal, 1 = verl
ose, 2 = debug)
```

4- Since version 5 no modules are available by default, we add them using the command **marketplace**.

But first, the module list should be updated with the command **marketplace refresh**.
And then we will search for module called hackertarget using the command
Marketplace search hackertarget

```
[recon-ng][default] > marketplace search hackertarget
[*] Searching module index for 'hackertarget'...

  +-------------------------------------------------------------------------+
  |            Path                | Version |    Status    | Updated  | D | K |
  +-------------------------------------------------------------------------+
  | recon/domains-hosts/hackertarget | 1.0    | not installed | 2019-06-24 |  |  |
  +-------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

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

5- To install the module “hackertarget” the command **marketplace install recon/domains-hosts/hackertarget** or **marketplace install hackertarget** can be used.

```
[recon-ng][default] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][default] >
```

6- To use a module the syntax is **modules load recon/domains-hosts/hackertarget** and the command **info** to display the options as seen below

```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.0

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE                 yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][hackertarget] >
```

7- To change the “SOURCE” option use the command **options set SOURCE** for example **options set SOURCE rapid7.com** to display the hosts of rapid7.com.
Type **run** to execute the module.

```
[recon-ng][default][hackertarget] > options set SOURCE rapid7.com
SOURCE => rapid7.com
[recon-ng][default][hackertarget] > run

----------
RAPID7.COM
----------
[*] [host] rapid7.com (13.249.47.238)
[*] [host] scanner1.labs.rapid7.com (71.6.233.2)
[*] [host] scanner2.labs.rapid7.com (71.6.233.129)
[*] [host] scanner3.labs.rapid7.com (31.24.231.211)
[*] [host] scanner4.labs.rapid7.com (31.24.231.223)
[*] [host] sonar.labs.rapid7.com (34.236.82.205)
...
```

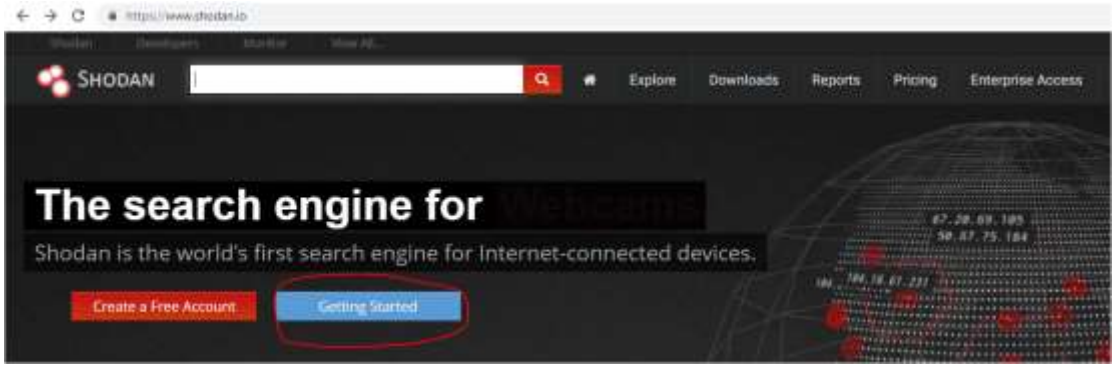
8- Now we have begun to populate our hosts. Typing show hosts will give you a summary of the resources discovered

Working with Shodan

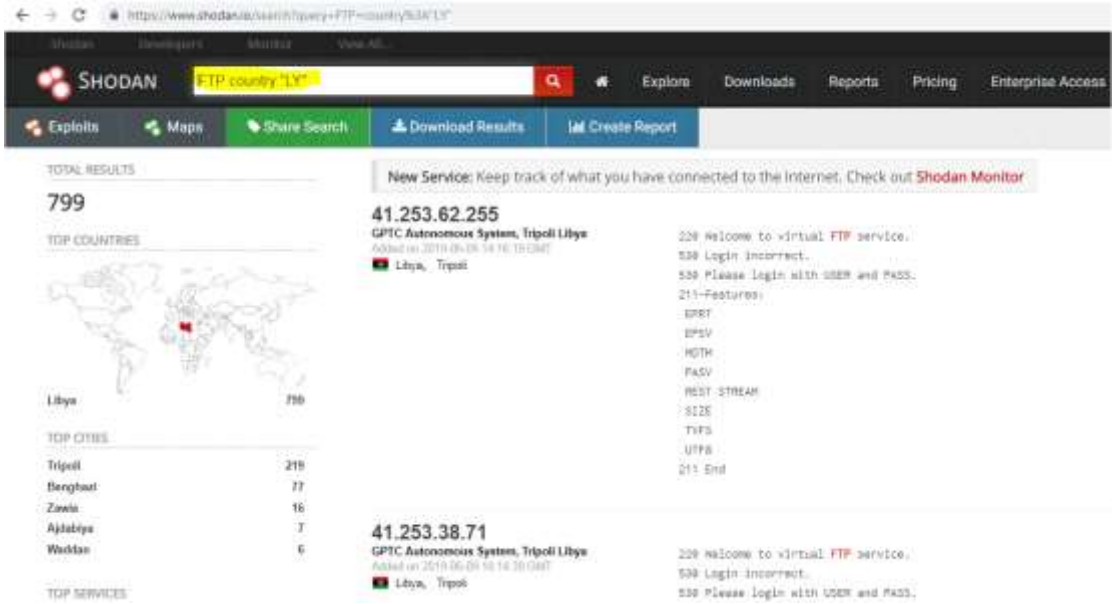
Step1: browsing https://www.shodan.io/

- 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

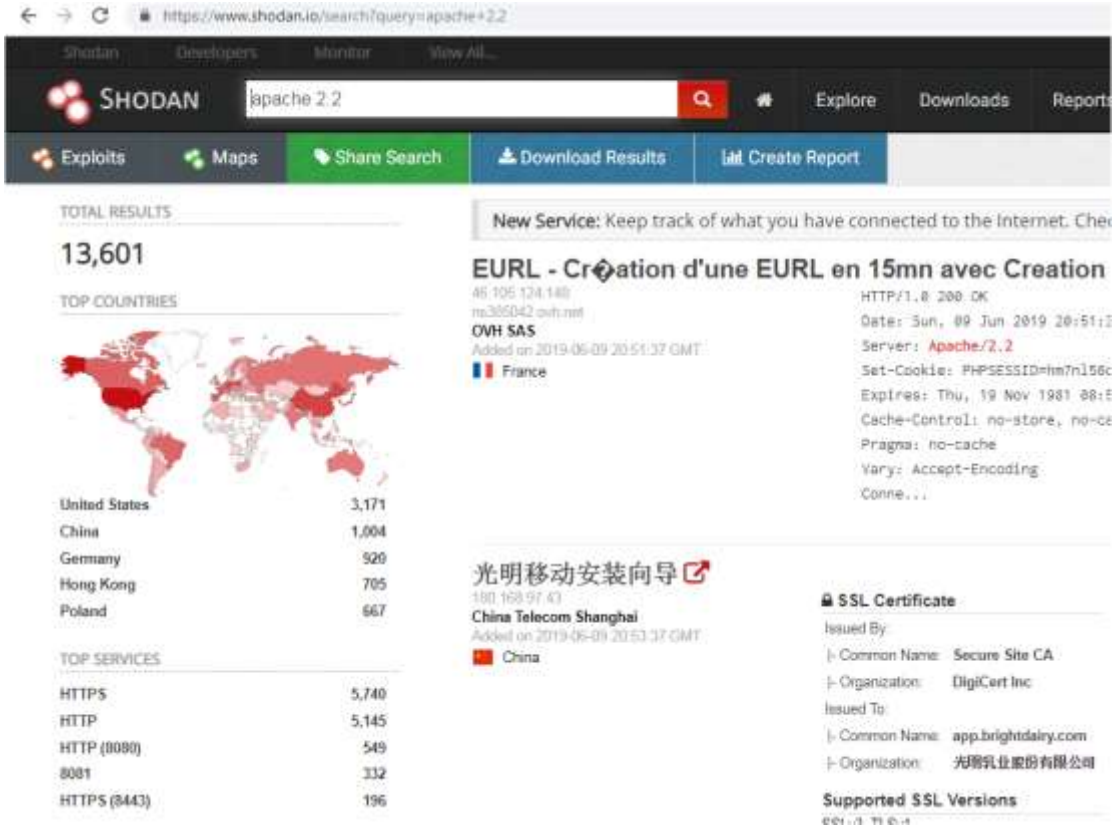


Step 3: exploring Shodan for example we looking for FTP server in Libya we will use filter FTP country: "LY" we found 799 FTP servers



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

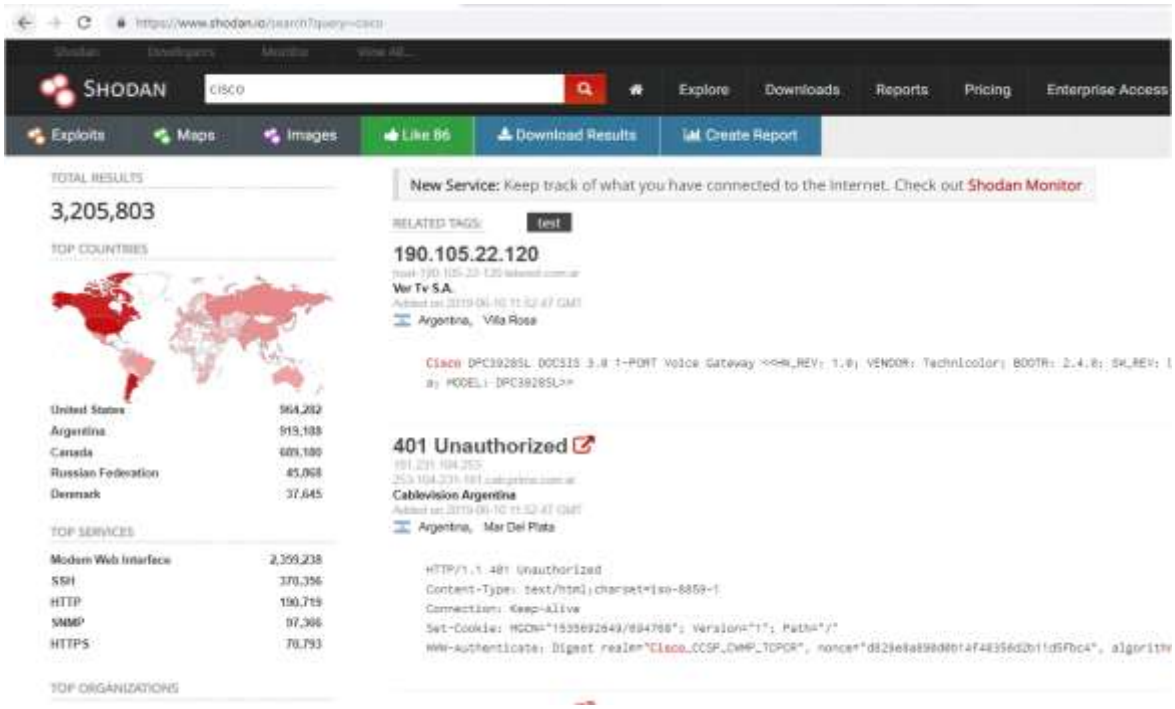
- Using SHODAN for penetration testing requires some basic knowledge of banners including HTTP status codes**.**
- Banners advertise service and version

HTTP Status Codes

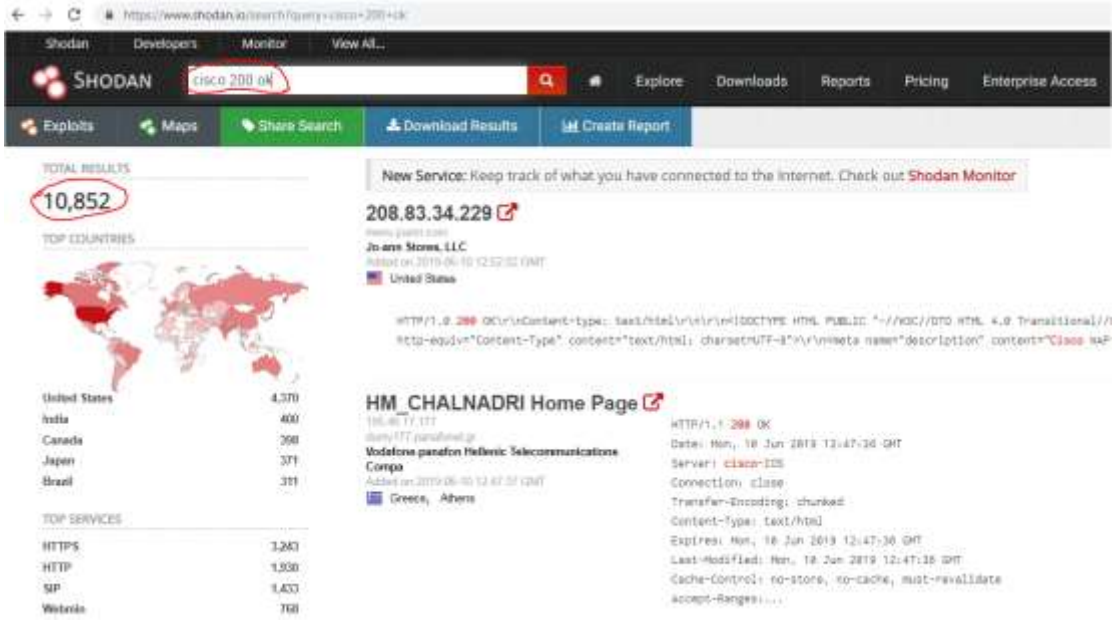
Status Code	Description
200 OK	Request succeeded
401 Unauthorized	Request requires authentication
403 Forbidden	Request is denied regardless of authentication

Case Study: Cisco Devices

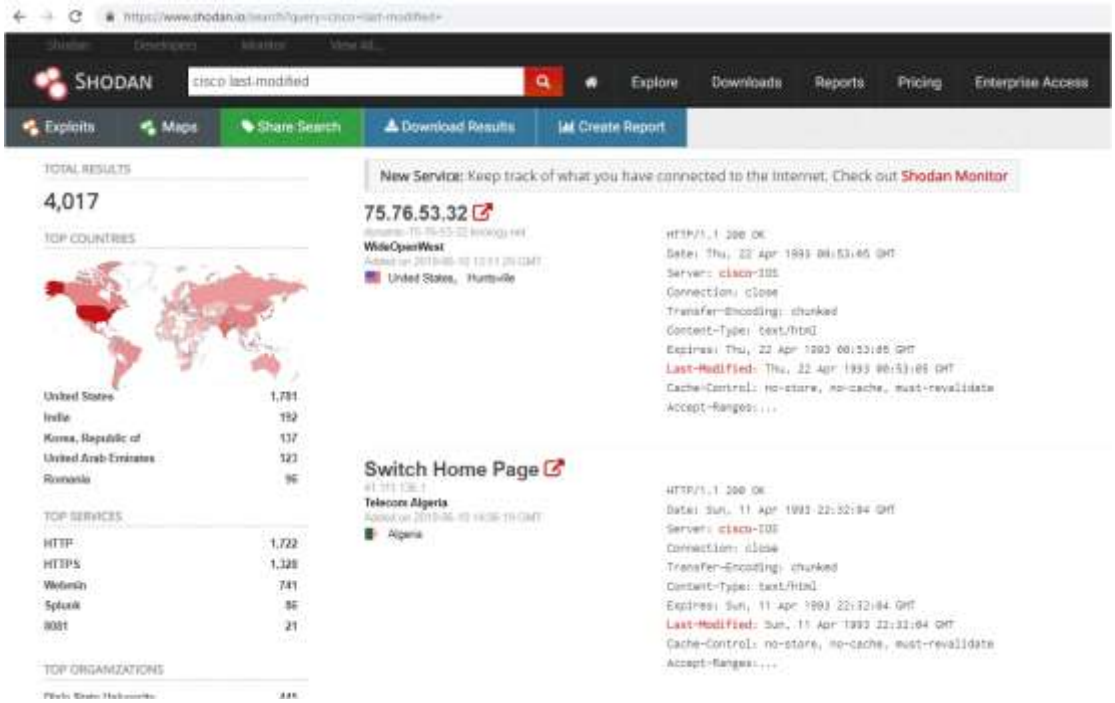
Step1: In shodan search write cisco and press enter



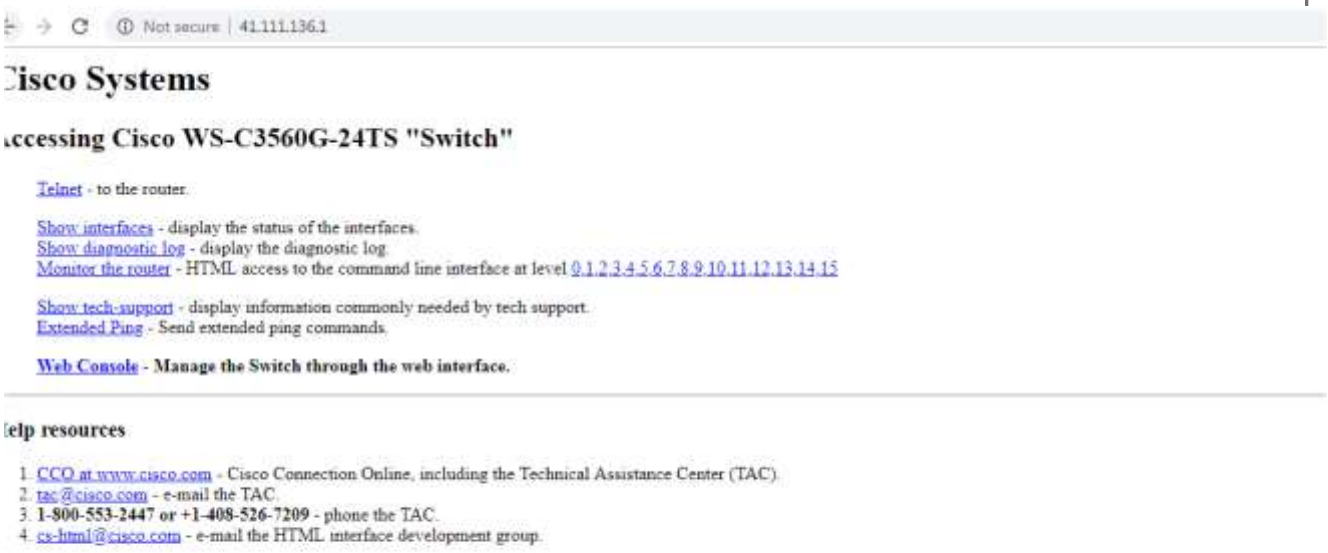
Step2: let us try using filter cisco 200 ok

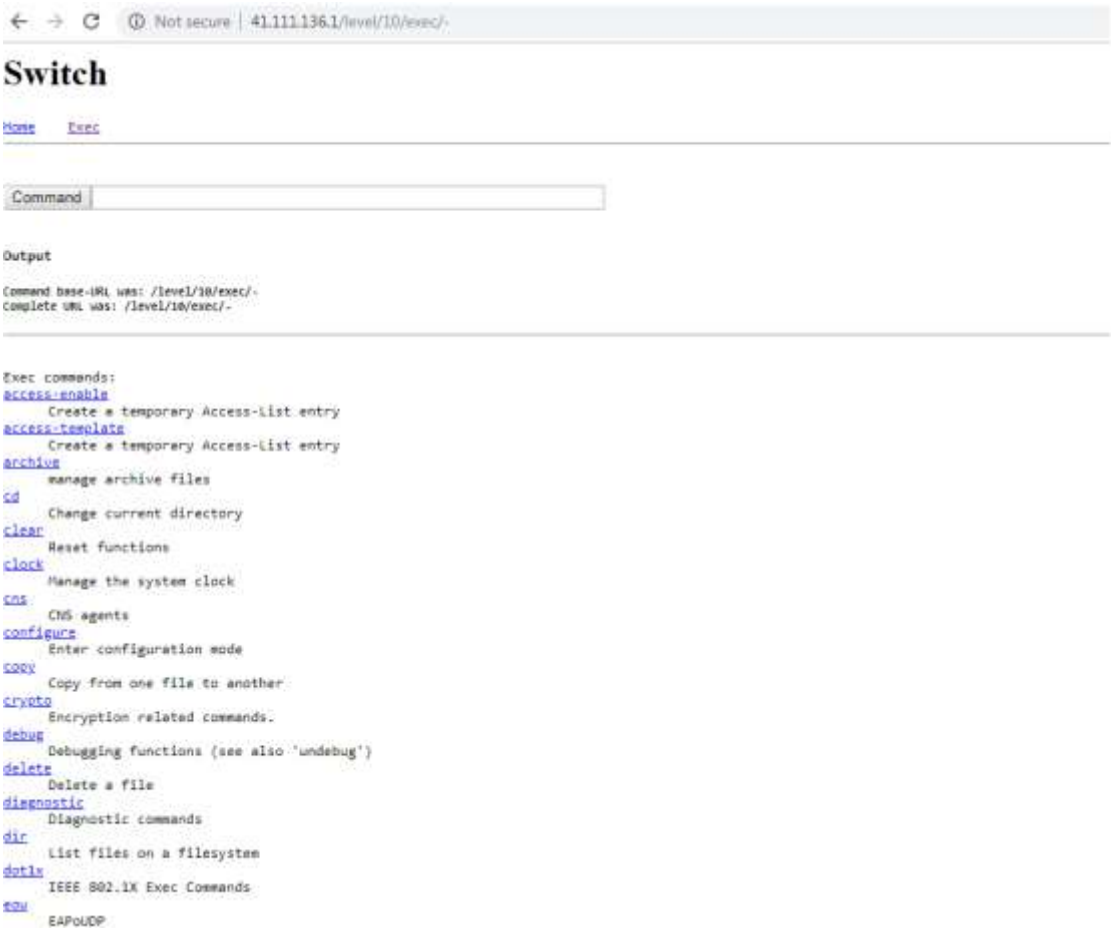


Step3: let us try cisco last modified



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

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

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 Bing:
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...
        Searching 200 results...
        Searching 250 results...
        Searching 300 results...
        Searching 350 results...
        Searching 400 results...
        Searching 450 results...
        Searching 500 results...
```

```
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

```
root@kali:~# theharvester -d micrsoft.com -l 200 -b linkedin

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 Linkedin..
```

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

[-] Searching in Linkedin..
        Searching 100 results..
        Searching 200 results..
Users from Linkedin:
-------------------
Tri Hua
Daniel Price - Director of IT - 343 Industries
Lisa Svensson
Jose Valencia
Travis Wright
Michel van Vliet - Cloud Solutions Specialist - Wortell
Wayne Joyce - Software Developer - TMW Systems
Karan Bajwa - Managing Director - IBM India Private Limited
Ed Dawson
Wenlei He - Software Engineer - Facebook
Jeff Merkle - Senior Partner - GRAPH Strategy
Suzie Harris - Senior Program Manager - Microsoft
Marco Heddes - Principal Architect - Microsoft
David Ku - Entrepreneur - Stealth AI company
Sara Schuster - Software Engineer II - Microsoft
Meron Fridman - Senior Consultant - Microsoft
Bruno Rangel - Analista de TI - MXM Sistemas
Konstantin Reverdatto - Senior Hardware Engineer - Microsoft
Jonny Bryan - Chief Of Staff - Unit4
Achindra Bhatnagar - Senior Software Engineer - Microsoft
-Michael Talbot- - Account Executive - Microsoft
Raju chandra Dey - Software Engineer - Microsoft
Phil Barnett - Account Technology Strategist - Microsoft
Delton C. - Game Developer - micrsoft
Alysha Arshad - Software Development Engineer - Microsoft
Jordan Ross - Program Manager - Microsoft
Harsh Vardhan - Software Development Engineer - Microsoft
Jason Panavich - Principal Engineer - Microsoft
Joe Lurie - Senior Product Marketing Manager - Microsoft
```