

# **Certified Ethical Hacking With Penetration Testing**

## **CEHWPT**

**LABS Course**

**LAB3 working with Reconnaissance tools**

**Prepared by Eng. Khaled Gamo**

**15-6-2019**

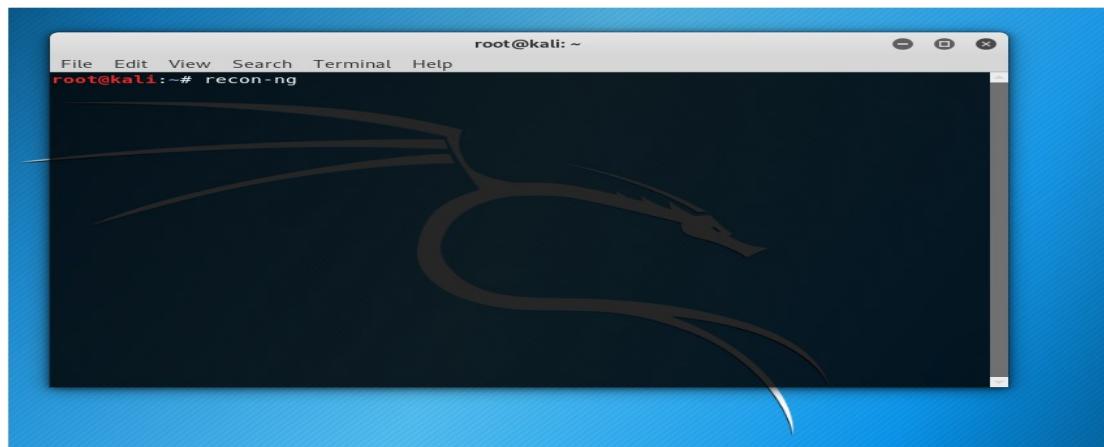
## LAB3 working with Reconnaissance tools

### 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.

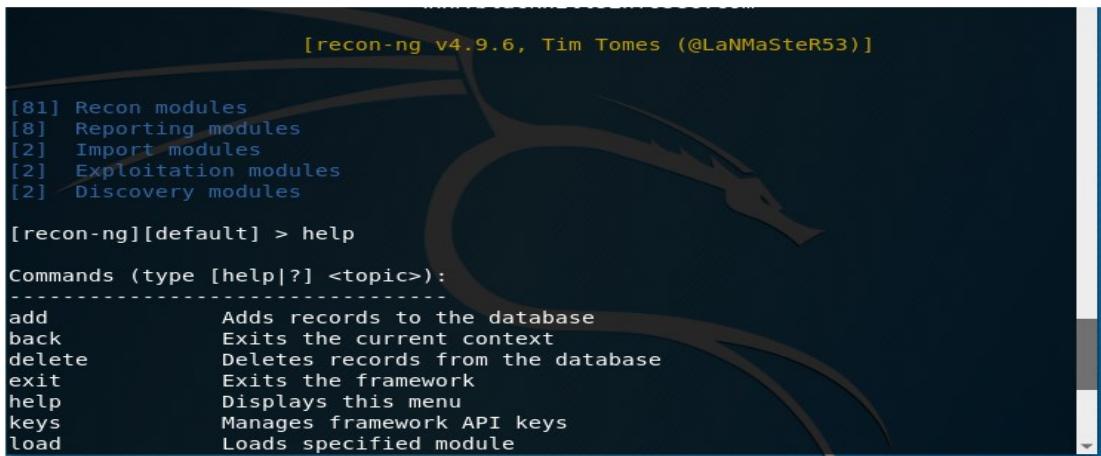
### Step 1: Starting Recon-ng

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

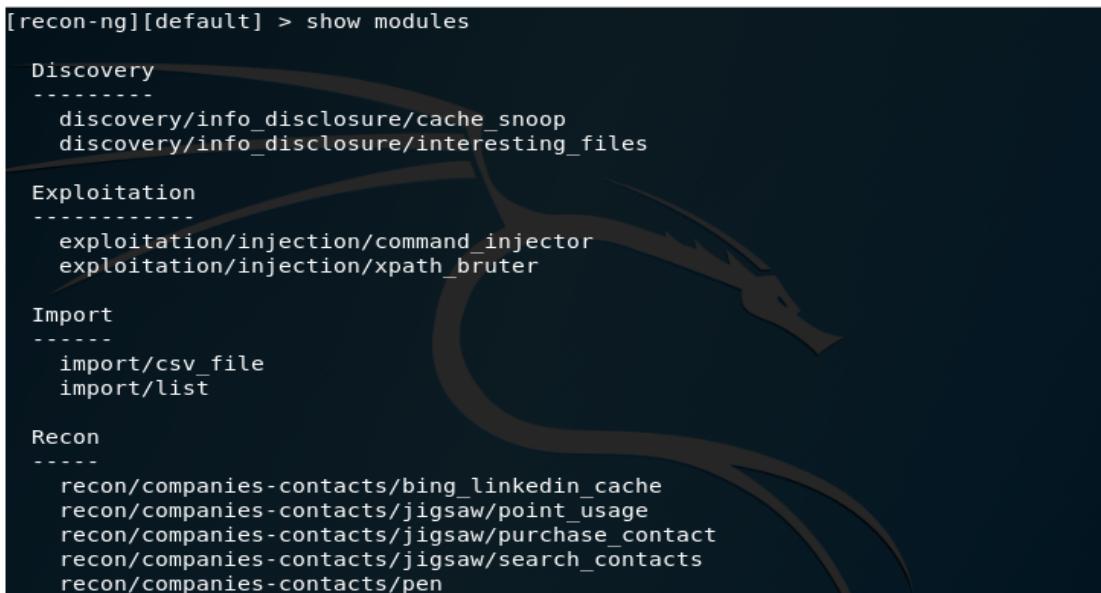


```
[recon-ng v4.9.6, Tim Tomes (@LaNMaSteR53)]
[81] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] > help
Commands (type [help|?] <topic>):
-----
add          Adds records to the database
back         Exits the current context
delete       Deletes records from the database
exit         Exits the framework
help         Displays this menu
keys         Manages framework API keys
load         Loads specified module
```

### Step 3: Showing Modules

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



```
[recon-ng][default] > show modules
Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

Exploitation
-----
exploitation/injection/command_injector
exploitation/injection/xpath_bruter

Import
-----
import/csv_file
import/list

Recon
-----
recon/companies-contacts/bing_linkedin_cache
recon/companies-contacts/jigsaw/point_usage
recon/companies-contacts/jigsaw/purchase_contact
recon/companies-contacts/jigsaw/search_contacts
recon/companies-contacts/pen
```

### 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**

Name	Value
bing_api	[REDACTED]
builtwith_api	[REDACTED]
censysio_id	[REDACTED]
censysio_secret	[REDACTED]
flickr_api	[REDACTED]
fullcontact_api	[REDACTED]
github_api	[REDACTED]
google_api	[REDACTED]
hashes_api	[REDACTED]
ipinfodb_api	[REDACTED]
ipstack_api	[REDACTED]
jigsaw_api	[REDACTED]
jigsaw_password	[REDACTED]
jigsaw_username	[REDACTED]
pwnedlist_api	[REDACTED]
pwnedlist_iv	[REDACTED]
pwnedlist_secret	[REDACTED]
shodan_api	[REDACTED]
twitter_api	[REDACTED]

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

```
[recon-ng][default] > keys add twitter_api 12345
[*] Key 'twitter_api' added.
[recon-ng][default] > keys list
```

bing_api	
builtwith_api	
censysio_id	
censysio_secret	
flickr_api	
fullcontact_api	
github_api	
google_api	
hashes_api	
ipinfodb_api	
ipstack_api	
jigsaw_api	
jigsaw_password	
jigsaw_username	
pwnedlist_api	
pwnedlist_iv	
pwnedlist_secret	
shodan_api	
twitter_api	12345
twitter_secret	
virustotal_api	

## 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.

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

Activity Summary	
Module	Runs
recon/domains-hosts/netcraft	3
recon/hosts-hosts/resolve	1

Results Summary	
Category	Quantity
Domains	3
Companies	0
Netblocks	0
Locations	0
Vulnerabilities	0
Ports	0
Hosts	240

**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

```
+-----+-----+
| 2   | kali.org | user_defined |
+-----+-----+
[*] 1 rows returned
recon-ng][newworkspace] > search domains
[*] Searching for 'domains'...
Recon
-----
recon/companies-domains/pen
recon/contacts-domains/migrate_contacts
recon/domains-companies/pen
recon/domains-contacts/metacrawler
recon/domains-contacts/pen
recon/domains-contacts/pgp_search
recon/domains-contacts/whois_pocs
recon/domains-credentials/pwnedlist/account_creds
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_creds
recon/domains-credentials/pwnedlist/domain_isowned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump
recon/domains-domains/brute_suffix
recon/domains-hosts/bing_domain_api
recon/domains-hosts/bing_domain_web
recon/domains-hosts/brute_hosts
recon/domains-hosts/builtwith
recon/domains-hosts/certificate_transparency
recon/domains-hosts/findsubdomains
recon/domains-hosts/google_site_web
recon/domains-hosts/hackerTarget
recon/domains-hosts/mx_spf_ip
recon/domains-hosts/netcraft
recon/domains-hosts/shodan_hostname
recon/domains-hosts/sst_san
recon/domains-hosts/threatcrowd
recon/domains-hosts/threatminer
recon/domains-vulnerabilities/ghdb
```

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

```
[recon-ng][newworkspace] > use recon/domains-hosts/netcraft
[recon-ng][newworkspace][netcraft] > show info

Name: Netcraft Hostname Enumerator
Path: modules/recon/domains-hosts/netcraft.py
Author: thrapt (thrapt@gmail.com)

Description:
  Harvests hosts from Netcraft.com. Updates the 'hosts' table with the results.

Options:
  Name      Current Value  Required  Description
  -----  -----
  SOURCE    default        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
```

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

```
[recon-ng][newworkspace][netcraft] > set SOURCE kali.org
SOURCE => kali.org
[recon-ng][newworkspace][netcraft] > run

-----
KALI.ORG
-----
[*] URL: http://searchdns.netcraft.com/?{'restriction': 'site+ends+with', 'host': 'kali.org'}
[*] [host] docs.kali.org (<blank>)
[*] [host] http.kali.org (<blank>)
[*] [host] cdimage.kali.org (<blank>)
[*] [host] security.kali.org (<blank>)
[*] [host] pkg.kali.org (<blank>)
[*] [host] de.docs.kali.org (<blank>)
[*] [host] archive-2.kali.org (<blank>)
[*] [host] fr.docs.kali.org (<blank>)
[*] [host] br.docs.kali.org (<blank>)
[*] [host] forums.kali.org (<blank>)
```

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
[*] cimage.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

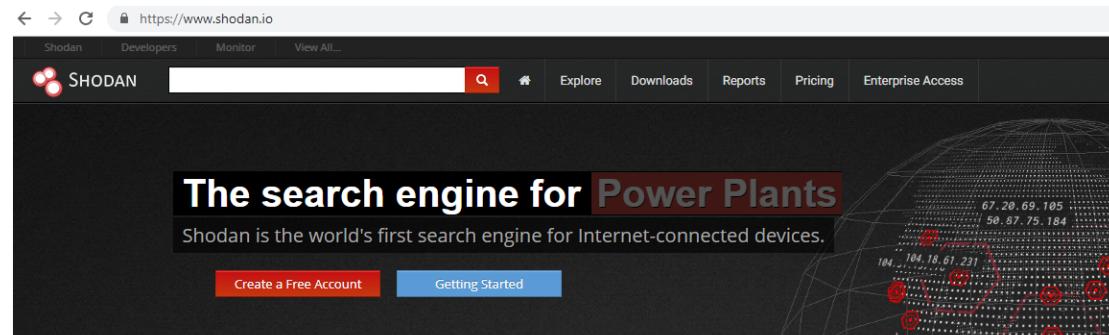
"use recon/domains-contacts/pgp\_search".

**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.

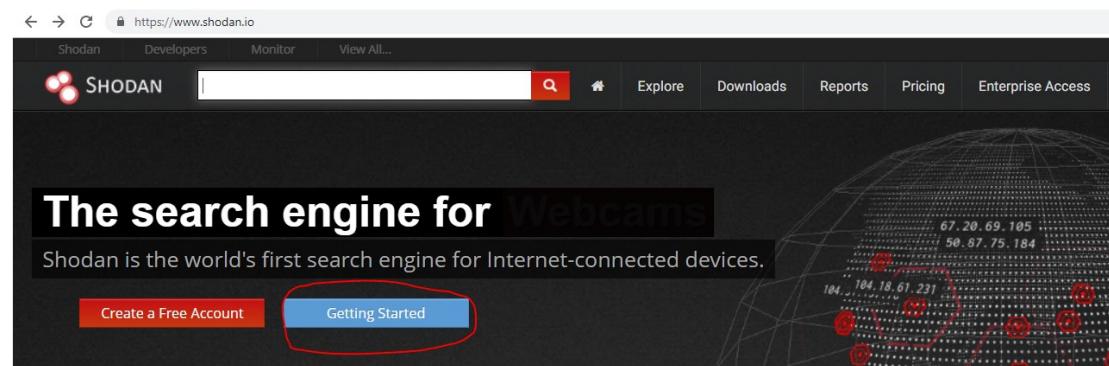
## Working with Shodan

**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

**TOTAL RESULTS**  
799

**TOP COUNTRIES**

Country	Count
Libya	799

**TOP CITIES**

City	Count
Tripoli	219
Benghazi	77
Zawia	16
Ajdabiya	7
Waddan	6

**TOP SERVICES**

**41.253.62.255**  
GPTC Autonomous System, Tripoli Libya  
Added on 2019-06-09 14:16:19 GMT  
Libya, Tripoli

220 Welcome to virtual **FTP** service.  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
UTF8  
211 End

**41.253.38.71**  
GPTC Autonomous System, Tripoli Libya  
Added on 2019-06-09 18:14:39 GMT  
Libya, Tripoli

220 Welcome to virtual **FTP** service.  
530 Login incorrect.  
530 Please login with USER and PASS.

**Step 3:** looking for Apache/2.2

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

**TOTAL RESULTS**  
13,601

**TOP COUNTRIES**

Country	Count
United States	3,171
China	1,004
Germany	920
Hong Kong	705
Poland	667

**TOP SERVICES**

Service	Count
HTTPS	5,740
HTTP	5,145
HTTP (8080)	549
8081	332
HTTPS (8443)	196

**EURL - Cr<sup>o</sup>ation d'une EURL en 15mn avec Creation**  
46.105.124.148  
ns385042.ovh.net  
OVH SAS  
Added on 2019-06-09 20:51:37 GMT  
France

HTTP/1.0 200 OK  
Date: Sun, 09 Jun 2019 20:51:37 GMT  
Server: **Apache/2.2**  
Set-Cookie: PHPSESSID=hm7nl56c  
Expires: Thu, 19 Nov 1981 08:56:16 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
Vary: Accept-Encoding  
Content-Type: text/html; charset=UTF-8

**光明移动安装向导**  
180.168.97.43  
China Telecom Shanghai  
Added on 2019-06-09 20:53:37 GMT  
China

**SSL Certificate**  
Issued By:  
- Common Name: Secure Site CA  
- Organization: DigiCert Inc  
Issued To:  
- Common Name: app.brightdairy.com  
- Organization: 光明乳业股份有限公司

**Supported SSL Versions**  
TLS 1.2 TLS 1.1

## 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

The screenshot shows the Shodan search interface with the query 'cisco' entered. The results page displays the following information:

- TOTAL RESULTS:** 3,205,803
- TOP COUNTRIES:** United States (964,282), Argentina (919,188), Canada (689,180), Russian Federation (45,868), Denmark (37,645).
- TOP SERVICES:** Modem Web Interface (2,359,238), SSH (370,356), HTTP (190,719), SNMP (97,366), HTTPS (70,793).
- TOP ORGANIZATIONS:** (not visible in the screenshot but present in the UI).
- Search Results:**
  - 190.105.22.120:** A detailed card for a Cisco DPC3928SL DOCSIS 3.0 1-PORT Voice Gateway located in Argentina, Villa Rosa. It was added on 2019-06-10 11:52:47 GMT. The card includes a map pin icon and a link to the device's details.
  - 401 Unauthorized:** A detailed card for a Cisco device with IP 181.231.104.253 located in Argentina, Mar Del Plata. It was added on 2019-06-10 11:52:47 GMT. The card includes a map pin icon and a link to the device's details.

## Step2: let us try using filter cisco +200 ok

<https://www.shodan.io/search?query=cisco+200+ok>

TOTAL RESULTS  
10,852

TOP COUNTRIES

COUNTRY	RESULTS
United States	4,370
India	400
Canada	398
Japan	371
Brazil	311

TOP SERVICES

SERVICE	RESULTS
HTTPS	3,243
HTTP	1,930
SIP	1,433
Webmin	768

208.83.34.229

menu.joann.com  
Jo-ann Stores, LLC  
Added on 2019-06-10 12:52:02 GMT  
United States

```
HTTP/1.0 200 OK\r\nContent-type: text/html\r\n\r\n<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//I\r\nhttp-equiv="Content-Type" content="text/html; charset=UTF-8">\r\n<meta name="description" content="Cisco WAP"
```

HM\_CHALNADRI Home Page

195.46.17.177  
dumy177.panafonet.gr  
Vodafone-panafon Hellenic Telecommunications  
Compa  
Added on 2019-06-10 12:47:37 GMT  
Greece, Athens

```
HTTP/1.1 200 OK\r\nDate: Mon, 10 Jun 2019 12:47:36 GMT\r\nServer: cisco-IOS\r\nConnection: close\r\nTransfer-Encoding: chunked\r\nContent-Type: text/html\r\nExpires: Mon, 10 Jun 2019 12:47:36 GMT\r\nLast-Modified: Mon, 10 Jun 2019 12:47:36 GMT\r\nCache-Control: no-store, no-cache, must-revalidate\r\nAccept-Ranges:...
```

## Step3: let us try cisco last modified

<https://www.shodan.io/search?query=cisco+last-modified+>

TOTAL RESULTS  
4,017

TOP COUNTRIES

COUNTRY	RESULTS
United States	1,781
India	192
Korea, Republic of	137
United Arab Emirates	123
Romania	96

TOP SERVICES

SERVICE	RESULTS
HTTP	1,722
HTTPS	1,328
Webmin	741
Splunk	86
8081	21

75.76.53.32

dynamic-75-76-53-32.knology.net  
WideOpenWest  
Added on 2019-06-10 13:51:29 GMT  
United States, Huntsville

```
HTTP/1.1 200 OK\r\nDate: Thu, 22 Apr 1993 00:53:05 GMT\r\nServer: cisco-IOS\r\nConnection: close\r\nTransfer-Encoding: chunked\r\nContent-Type: text/html\r\nExpires: Thu, 22 Apr 1993 00:53:05 GMT\r\nLast-Modified: Thu, 22 Apr 1993 00:53:05 GMT\r\nCache-Control: no-store, no-cache, must-revalidate\r\nAccept-Ranges:...
```

Switch Home Page

41.111.136.1  
Telecom Algeria  
Added on 2019-06-10 14:06:19 GMT  
Algeria

```
HTTP/1.1 200 OK\r\nDate: Sun, 11 Apr 1993 22:32:04 GMT\r\nServer: cisco-IOS\r\nConnection: close\r\nTransfer-Encoding: chunked\r\nContent-Type: text/html\r\nExpires: Sun, 11 Apr 1993 22:32:04 GMT\r\nLast-Modified: Sun, 11 Apr 1993 22:32:04 GMT\r\nCache-Control: no-store, no-cache, must-revalidate\r\nAccept-Ranges:...
```

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

The screenshot shows a web browser window with the following details:

- Address bar: Not secure | 41.111.136.1
- Title: Cisco Systems
- Section: Accessing Cisco WS-C3560G-24TS "Switch"
- Text:
  - [Telnet](#) - to the router.
  - [Show interfaces](#) - display the status of the interfaces.
  - [Show diagnostic log](#) - display the diagnostic log.
  - [Monitor the router](#) - HTML access to the command line interface at level [0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15](#).
  - [Show tech-support](#) - display information commonly needed by tech support.
  - [Extended Ping](#) - Send extended ping commands.
  - [Web Console](#) - Manage the Switch through the web interface.

#### Help resources

1. [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. [tac@cisco.com](#) - e-mail the TAC.
3. [1-800-553-2447 or +1-408-526-7209](#) - phone the TAC.
4. [cs-html@cisco.com](#) - e-mail the HTML interface development group.

← → ⌂ ⓘ 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.

```
root@kali:~# theharvester
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.

*****
*   results.html
*****
* theHarvester Ver. 3.0.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****


Usage: theharvester options

-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
     google, google-certificates, googleCSE, googleplus, google-profiles,
     hunter, linkedin, netcraft, pgp, threatcrowd,
     twitter, vhost, virustotal, yahoo, all
-g: use Google dorking instead of normal Google search
-s: start in result number X (default: 0)
-v: verify host name via DNS resolution and search for virtual hosts
-f: save the results into an HTML and XML file (both)
-n: perform a DNS reverse query on all ranges discovered
-c: perform a DNS brute force for the domain name
-t: perform a DNS TLD expansion discovery
-e: use this DNS server
-p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
-l: limit the number of results to work with(Bing goes from 50 to 50 results,
     Google 100 to 100, and PGP doesn't use this option)
-h: use SHODAN database to query discovered hosts
```



```
Harvesting results [sword1.txt]
No IP addresses found

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

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

```
root@kali:~# theharvester -d microsoft.com -l 500 -b google
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.

*****
*          ^__^
*       /  \_\_\
*      o   o\_\_\_
*      ||----w |
*      ||     ||----w |
*      *     ||     ||----w |
*          *     ||     ||----w |
*               ||     ||----w |
*   *       theHarvester Ver. 3.0.6
*   *       Coded by Christian Martorella
*   *       Edge-Security Research
*   *       cmartorella@edge-security.com
****

found supported engines
[-] Starting harvesting process for domain: microsoft.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@microsoft.com  
msnhst@microsoft.com  
account-security-noraply@microsoft.com  
josegonzalez@microsoft.com  
rlawrence@microsoft.com  
mcphelp@microsoft.com  
inclusive@design@microsoft.com  
zdeng@online.microsoft.com  
v-siwils@microsoft.com  
houwen.peng@microsoft.com  
leans@microsoft.com  
dinei@microsoft.com  
scottr@microsoft.com  
edwardgates@microsoft.com  
morons@microsoft.com  
quarantine@messaging.microsoft.com  
  
[+] Hosts found in search engines:  
-----  
  
Total hosts: 24  
  
[-] Resolving hostnames IPs...  
  
Account.microsoft.com:empty  
XXX.microsoft.com:empty  
account.microsoft.com:empty  
connect.microsoft.com:empty  
demos.microsoft.com:empty  
docs.microsoft.com:empty  
fareast.corp.microsoft.com:empty  
go.microsoft.com:empty  
login.microsoft.com:empty  
messaging.microsoft.com:empty  
msdn.microsoft.com:empty  
office.microsoft.com:empty  
online.microsoft.com:empty
```

