Searching Shodan For Fun And Profit

Sajal Verma

SEARCHING SHODAN FOR FUN AND PROFIT

Author: Sajal Verma @sajalpentest (sajalverma007786@gmail.com)

Abstract:

This paper act as a guide for penetration testers and security folks who want to use Shodan and helps them to understand how it can be used it for security auditing purposes. This paper also outlines the procedure and explains the methods to find various vulnerable services and devices located on the internet. It helps to explain the basic filters that could be used by Shodan and its integration with other tools .It can be mainly used for reconnaissance phase of penetration testing.

Introduction:

Shodan is basically a search engine which helps to find (routers, switches, Scada etc.) mainly vulnerable systems on the internet .It is widely known as Google for hackers. It was launched in 2009 by computer programmer John Matherly. It is mainly a search engine of service banners in which metadata (data about data) is sent from the server to client. Shodan currently probes for 50+ ports.

What devices can Shodan really find:

1) Servers

2) Routers

3) Switches

4) Printers on public ip

5) Webcams

6) Gas station pumps

7) Voip phones And all Scada devices **Working of Shodan**:

1) User searches for a particular item.

2) Shodan probes for ports and captures the resulting banners.

3) Now, Shodan indexes the captured banners.

4) After indexing,it displays the results.

Difference between Shodan and google:

In Google,the google crawler/spider crawls for data on the web pages and then creates a index of web content and then displays the results according to the page rank which in turn depends on a number of factors. Shodan mainly looks for ports and then grabs the resulting banners and indexes them. And finally, it displays the results. It does not index web content (the key point) like google and thus it is a search engine of banners.

Figure 1.Shodan search working

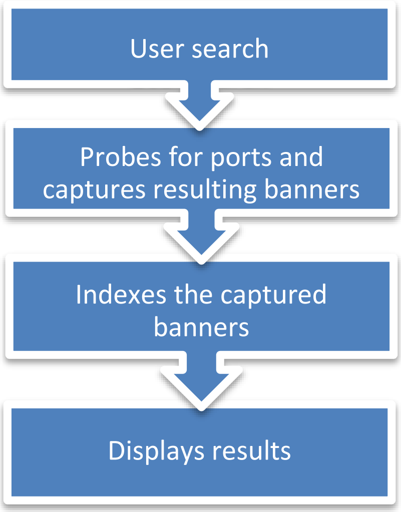
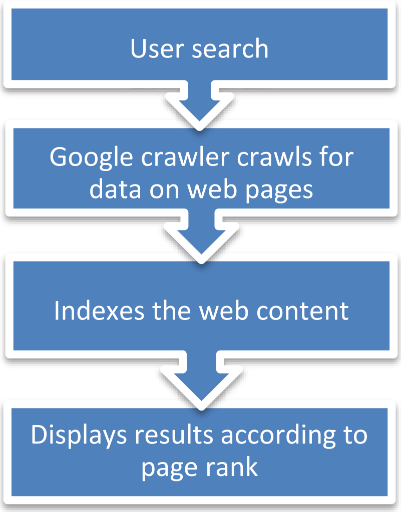

User search
Probes for ports and captures resulting banners
Indexes the captured banners
Displays results

Figure 2. Google search working


User search
Google crawler crawls for data on web pages
Indexes the web content
Displays results according to page rank

Basic filters:

City: The 'city' filter is used to find devices that are located in that particular city.

Eg:**iis city:New York**

Country: The 'country' filter is used devices running in that particular country.

Eg:iis country: United States

Port: The 'port' filter narrows the search by searching for specified ports.

Eg. **https port:443**

Os: The 'os' filter is used to find specific operating systems.

Eg: **microsoft-iis os:"windows 2003"**

Geo: The 'geo' filter according to certain longitudes and latitudes that are within a given radius. Only 2 3 parameters are allowed and 3 parameter by default is the radius which is 5 km.

Eg: **apache geo:42.9693,-74.1224**

Net: The 'net' filter is used to find devices according to certain ip address and subnet mask

Eg: **iis net:216.0.0.0/16**

Hostname: The 'hostname' filter always searches host containing a particular hostname.

Eg: **Akamai hostname:.com**

After and Before: The 'after' and 'before' filter helps you to devices after and before a particular date. The format allowed is

dd/mm/yyyy dd-mm-yy

Eg: apache before:1/01/2014

nginx after:1/01/2014

Note: Most of the filters will work when you are logged in.

Shodan's integration with other tools:

1) Integration with **Maltego**

Requirements: Download **Maltego** from

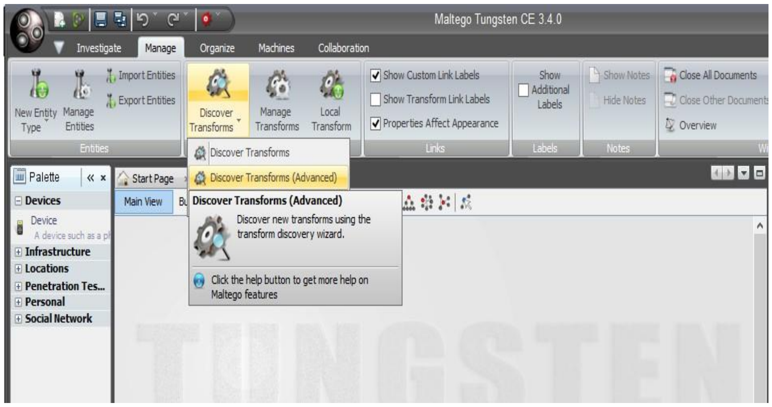
http://www.paterva.com/web6/products/download.php

and Shodan maltego entities from **https://static.Shodan.io/downloads/Shodan-maltego-entities.mtz**

Usage:

i) After installing maltego,select ‘Manage Entities’ in the ‘Manage tab’ and select ‘import’.

ii) Select ‘transforms’ and then ‘advanced’

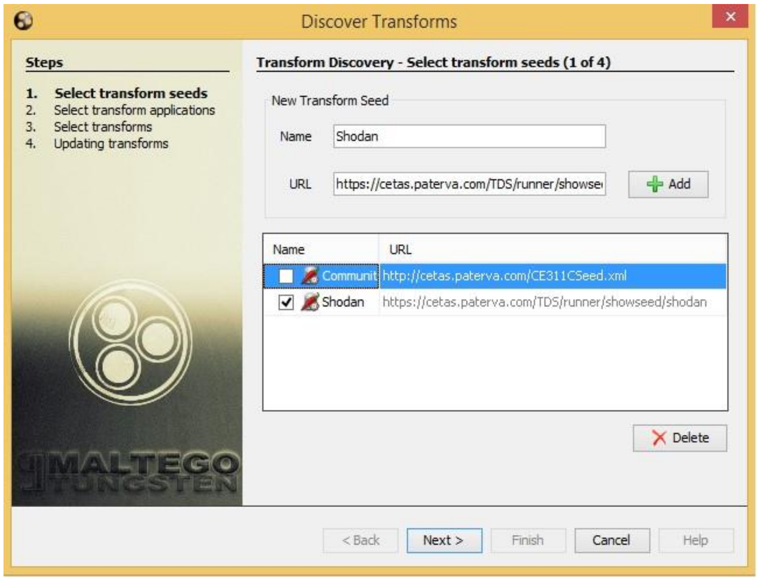


Discover Transforms (Advanced)

Discover new transforms using the transform discovery wizard.

Click the help button to get more help on Maltego features

iii) Now we have do add the Shodan seed by putting **https://cetas.paterva.com/TDS/runner/showseed/Shodan**



Steps

1. **Select transform seeds**
2. Select transform applications
3. Select transforms
4. Updating transforms

Transform Discovery - Select transform seeds (1 of 4)

New Transform Seed

Name: Shodan

URL: https://cetas.paterva.com/TDS/runner/showse

Name	URL
□ Communit	http://cetas.paterva.com/CE311CSeed.xml
☑ Shodan	https://cetas.paterva.com/TDS/runner/showseed/shodan

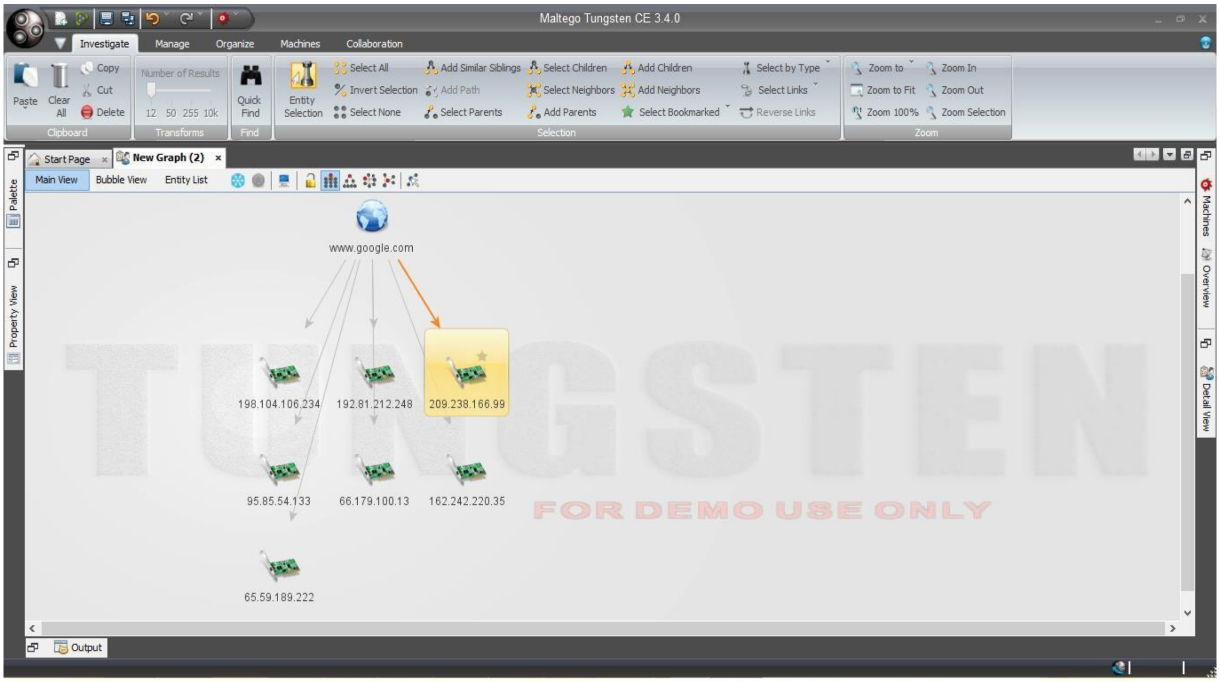
iv) Finally we get a screen ,the transforms and entities have been successfully installed.

It includes:

5 Transforms namely:

i)searchShodan
ii)searchShodanByDomain
iii)searchShodanByNetblock
iv)toShodanHost v)searchExploits

2 Entities namely:
i) Service
ii)Exploit
Here is a screen shot of the transform**(searchShodanByDomain**) performed on **google.com**



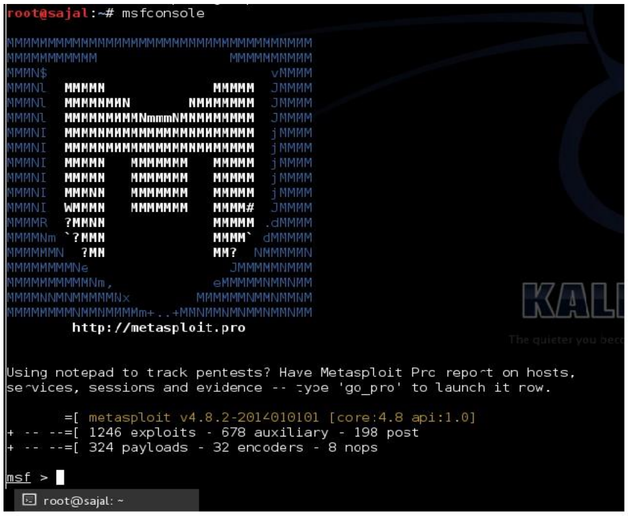
Note:

You can perform Shodan transforms in maltego when you have the API keys and you will get the API keys by logging into your Shodan account.

2) Integration with **Metasploit**

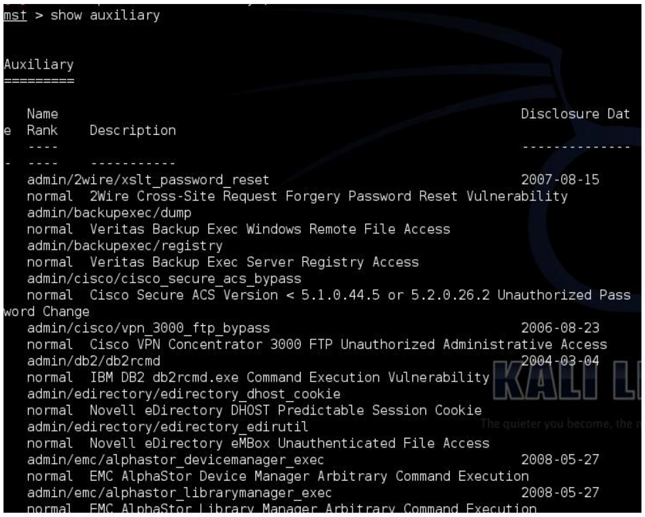
Usage:

i) Open Metasploit framework in Kali/Backtrack Box



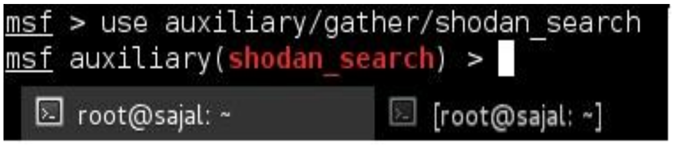
```
root@sajal:~# msfconsole

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        http://metasploit.pro


Using notepad to track pentests? Have Metasploit Prc repo-t on hosts,
se-vices, sessions and evidence -- type 'go_pro' to launch it row.

       =[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --=[ 1246 exploits - 678 auxiliary - 198 post
+ -- --=[ 324 payloads - 32 encoders - 8 nops

msf > █
```

ii.)Type show auxiliary in the console



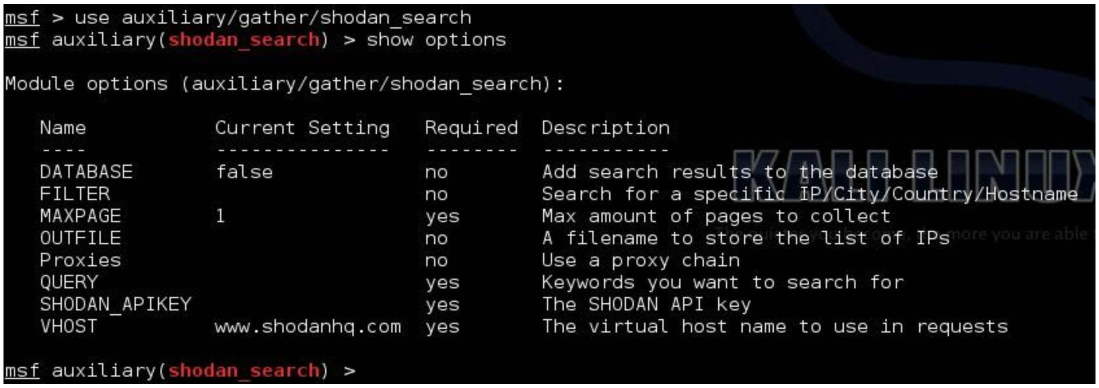
```
mst > show auxiliary


Auxiliary
=========

   Name                                                            Disclosure Dat
e  Rank    Description
   ----                                                            --------------
-  ----    -----------
   admin/2wire/xslt_password_reset                                 2007-08-15
   normal  2Wire Cross-Site Request Forgery Password Reset Vulnerability
   admin/backupexec/dump
   normal  Veritas Backup Exec Windows Remote File Access
   admin/backupexec/registry
   normal  Veritas Backup Exec Server Registry Access
   admin/cisco/cisco_secure_acs_bypass
   normal  Cisco Secure ACS Version < 5.1.0.44.5 or 5.2.0.26.2 Unauthorized Pass
word Change
   admin/cisco/vpn_3000_ftp_bypass                                 2006-08-23
   normal  Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
   admin/db2/db2rcmd                                               2004-03-04
   normal  IBM DB2 db2rcmd.exe Command Execution Vulnerability
   admin/edirectory/edirectory_dhost_cookie
   normal  Novell eDirectory DHOST Predictable Session Cookie
   admin/edirectory/edirectory_edirutil
   normal  Novell eDirectory eMBox Unauthenticated File Access
   admin/emc/alphastor_devicemanager_exec                          2008-05-27
   normal  EMC AlphaStor Device Manager Arbitrary Command Execution
   admin/emc/alphastor_librarymanager_exec                         2008-05-27
   normal  EMC AlphaStor Library Manager Arbitrary Command Execution
```

iii)Using the module **<u>auxiliary/gather/Shodansearch</u>**



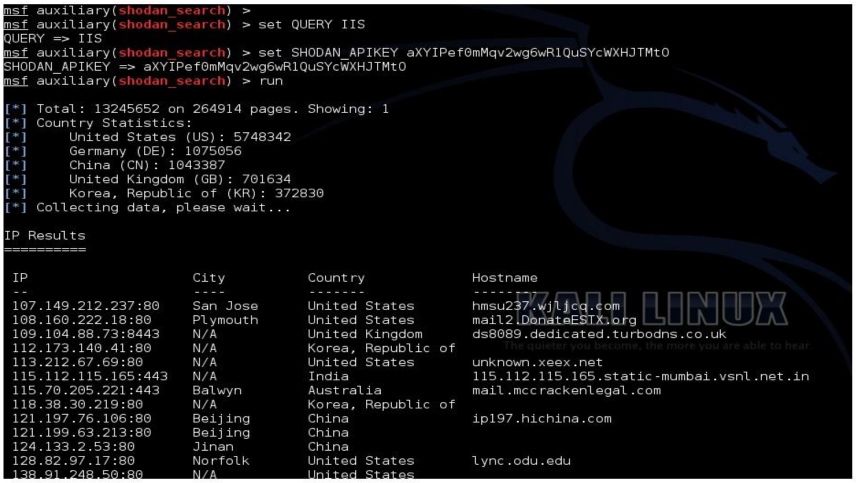
```
msf > use auxiliary/gather/shodan_search
msf auxiliary(shodan_search) > █
```

iv) Now, we will see the parameters required by the auxiliary by using **show options.**

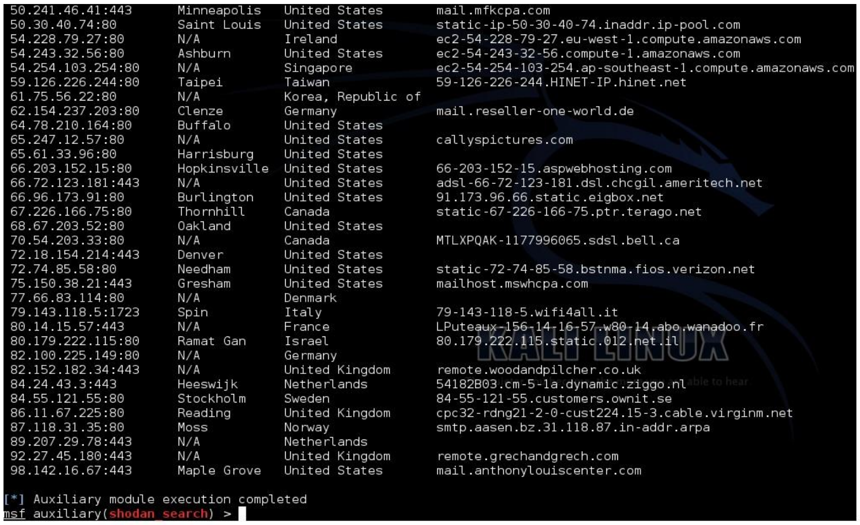


```
msf > use auxiliary/gather/shodan_search
msf auxiliary(shodan_search) > show options

Module options (auxiliary/gather/shodan_search):

   Name           Current Setting   Required  Description
   ----           ---------------   --------  -----------
   DATABASE       false             no        Add search results to the database
   FILTER                           no        Search for a specific IP/City/Country/Hostname
   MAXPAGE        1                 yes       Max amount of pages to collect
   OUTFILE                          no        A filename to store the list of IPs
   Proxies                          no        Use a proxy chain
   QUERY                            yes       Keywords you want to search for
   SHODAN_APIKEY                    yes       The SHODAN API key
   VHOST          www.shodanhq.com  yes       The virtual host name to use in requests

msf auxiliary(shodan_search) >
```

v.) We need to set query to IIS to search for IIS servers and the API key which we get when we log into our Shodan account.Now we execute it by the Run command.



```
msf auxiliary(shodan_search) >
msf auxiliary(shodan_search) > set QUERY IIS
QUERY => IIS
msf auxiliary(shodan_search) > set SHODAN_APIKEY aXYIPef0mMqv2wg6wR1QuSYcWXHJTMt0
SHODAN_APIKEY => aXYIPef0mMqv2wg6wR1QuSYcWXHJTMt0
msf auxiliary(shodan_search) > run

[*] Total: 13245652 on 264914 pages. Showing: 1
[*] Country Statistics:
[*]     United States (US): 5748342
[*]     Germany (DE): 1075056
[*]     China (CN): 1043387
[*]     United Kingdom (GB): 701634
[*]     Korea, Republic of (KR): 372830
[*] Collecting data, please wait...

IP Results
==========

 IP                     City          Country             Hostname
 --                     ----          -------             --------
 107.149.212.237:80     San Jose      United States       hmsu237.wjljcq.com
 108.160.222.18:80      Plymouth      United States       mail2.DonateESTX.org
 109.104.88.73:8443     N/A           United Kingdom      ds8089.dedicated.turbodns.co.uk
 112.173.140.41:80      N/A           Korea, Republic of
 113.212.67.69:80       N/A           United States       unknown.xeex.net
 115.112.115.165:443    N/A           India               115.112.115.165.static-mumbai.vsnl.net.in
 115.70.205.221:443     Balwyn        Australia           mail.mccrackenlegal.com
 118.38.30.219:80       N/A           Korea, Republic of
 121.197.76.106:80      Beijing       China               ip197.hichina.com
 121.199.63.213:80      Beijing       China
 124.133.2.53:80        Jinan         China
 128.82.97.17:80        Norfolk       United States       lync.odu.edu
 138.91.248.50:80       N/A           United States
```

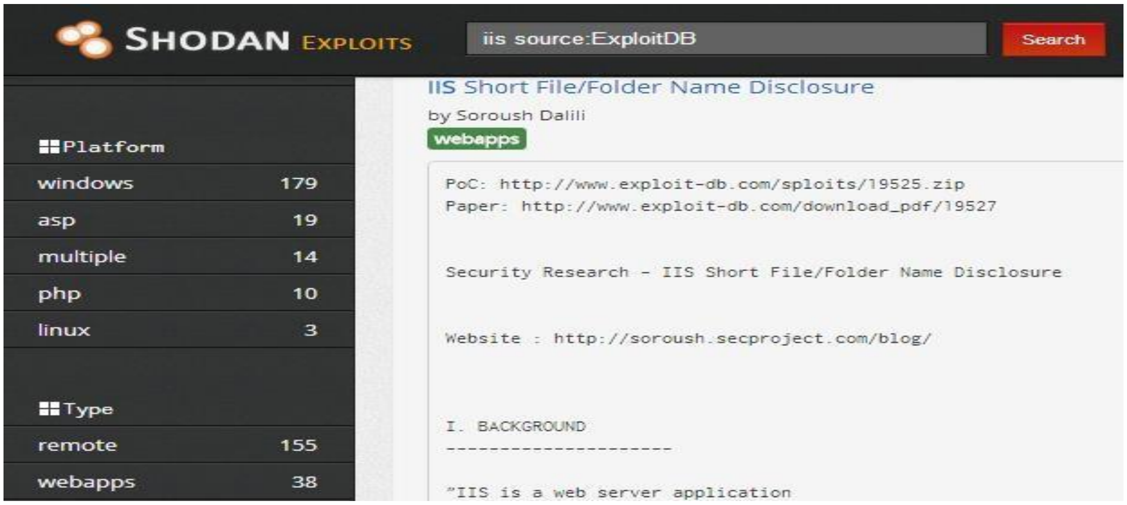


```
 50.241.46.41:443      Minneapolis   United States      mail.mfkcpa.com
 50.30.40.74:80        Saint Louis   United States      static-ip-50-30-40-74.inaddr.ip-pool.com
 54.228.79.27:80       N/A           Ireland            ec2-54-228-79-27.eu-west-1.compute.amazonaws.com
 54.243.32.56:80       Ashburn       United States      ec2-54-243-32-56.compute-1.amazonaws.com
 54.254.103.254:80     N/A           Singapore          ec2-54-254-103-254.ap-southeast-1.compute.amazonaws.com
 59.126.226.244:80     Taipei        Taiwan             59-126-226-244.HINET-IP.hinet.net
 61.75.56.22:80        N/A           Korea, Republic of
 62.154.237.203:80     Clenze        Germany            mail.reseller-one-world.de
 64.78.210.164:80      Buffalo       United States
 65.247.12.57:80       N/A           United States      callyspictures.com
 65.61.33.96:80        Harrisburg    United States
 66.203.152.15:80      Hopkinsville  United States      66-203-152-15.aspwebhosting.com
 66.72.123.181:443     N/A           United States      adsl-66-72-123-181.dsl.chcgil.ameritech.net
 66.96.173.91:80       Burlington    United States      91.173.96.66.static.eigbox.net
 67.226.166.75:80      Thornhill     Canada             static-67-226-166-75.ptr.terago.net
 68.67.203.52:80       Oakland       United States
 70.54.203.33:80       N/A           Canada             MTLXPQAK-1177996065.sdsl.bell.ca
 72.18.154.214:443     Denver        United States
 72.74.85.58:80        Needham       United States      static-72-74-85-58.bstnma.fios.verizon.net
 75.150.38.21:443      Gresham       United States      mailhost.mswhcpa.com
 77.66.83.114:80       N/A           Denmark
 79.143.118.5:1723     Spin          Italy              79-143-118-5.wifi4all.it
 80.14.15.57:443       N/A           France             LPuteaux-156-14-16-57.w80-14.abo.wanadoo.fr
 80.179.222.115:80     Ramat Gan     Israel             80.179.222.115.static.012.net.il
 82.100.225.149:80     N/A           Germany
 82.152.182.34:443     N/A           United Kingdom     remote.woodandpilcher.co.uk
 84.24.43.3:443        Heeswijk      Netherlands        54182B03.cm-5-1a.dynamic.ziggo.nl
 84.55.121.55:80       Stockholm     Sweden             84-55-121-55.customers.ownit.se
 86.11.67.225:80       Reading       United Kingdom     cpc32-rdng21-2-0-cust224.15-3.cable.virginm.net
 87.118.31.35:80       Moss          Norway             smtp.aasen.bz.31.118.87.in-addr.arpa
 89.207.29.78:443      N/A           Netherlands
 92.27.45.180:443      N/A           United Kingdom     remote.grechandgrech.com
 98.142.16.67:443      Maple Grove   United States      mail.anthonylouiscenter.com

[*] Auxiliary module execution completed
msf auxiliary(shodan_search) >
```

Basically the **auxiliary/gather/Shodan_search** module queries the Shodan API to query the database to search for the first 50 IP addresses. The limit of 50 IP address can be increased to 10,000 IP addresses by getting unlimited API keys by purchasing it from our Shodan account.

Components of Shodan:

1)**Exploits**: Shodan Exploits can be used to find exploits for various os, servers, platforms, applications etc present on ExploitDB or Metasploit.



iis source:ExploitDB

Platform

windows	179
asp	19
multiple	14
php	10
linux	3

Type

remote	155
webapps	38

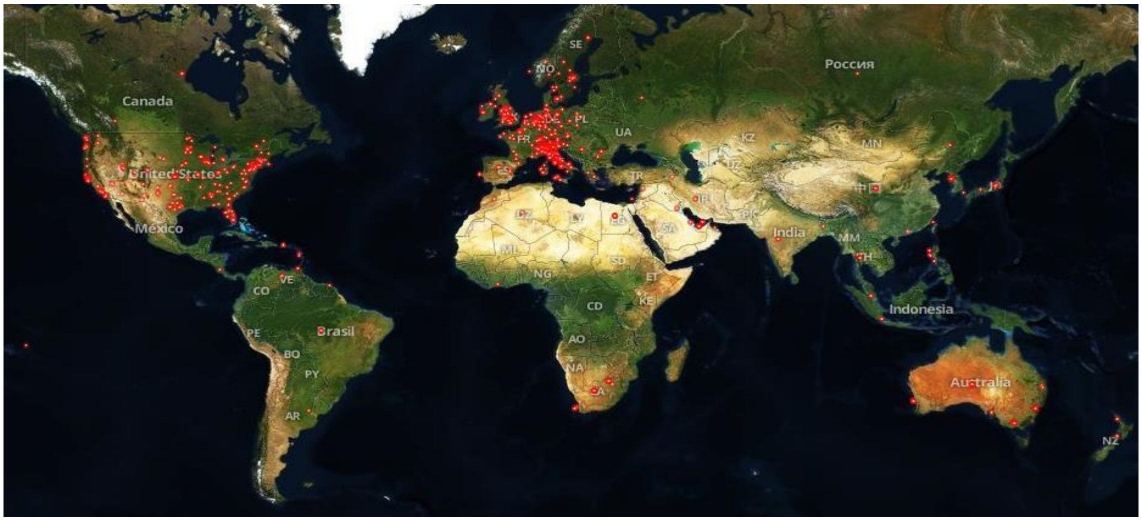
IIS Short File/Folder Name Disclosure

by Soroush Dalili

webapps

```
PoC: http://www.exploit-db.com/sploits/19525.zip
Paper: http://www.exploit-db.com/download_pdf/19527


Security Research - IIS Short File/Folder Name Disclosure


Website : http://soroush.secproject.com/blog/



I. BACKGROUND
---------------------

"IIS is a web server application
```

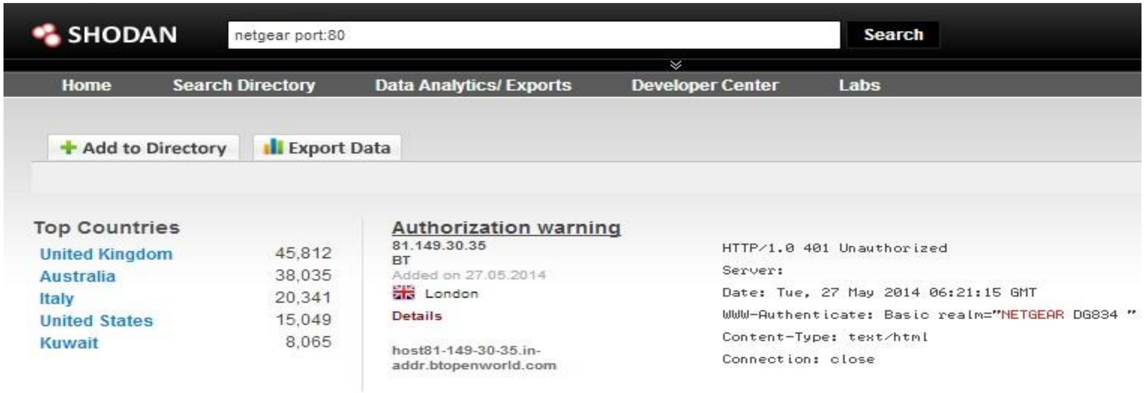
2)**Maps**: Shodan maps is a paid service and you need to pay for it before using. We can see the Shodan results on a map in a easy and convenient manner.It has three kind of map views namely Satellite, Street View (Light) and Street View (Dark).It can show upto 1000 results on the screen at a time.



3)**Scanhubs**: Shodan Scanhubs can be used to create an to use to create a search of raw networks scans.Scanhubs supports tools like Nmap and Masscan.To use Scanhub .We have to set the tool(nmap/masscan) to give its output in XML format and then upload it to the Scanhub repository to get the results.Unfortunately this is also a paid component of Shodan.

<u>Some Test Cases</u>:

1) **Netgear devices**:



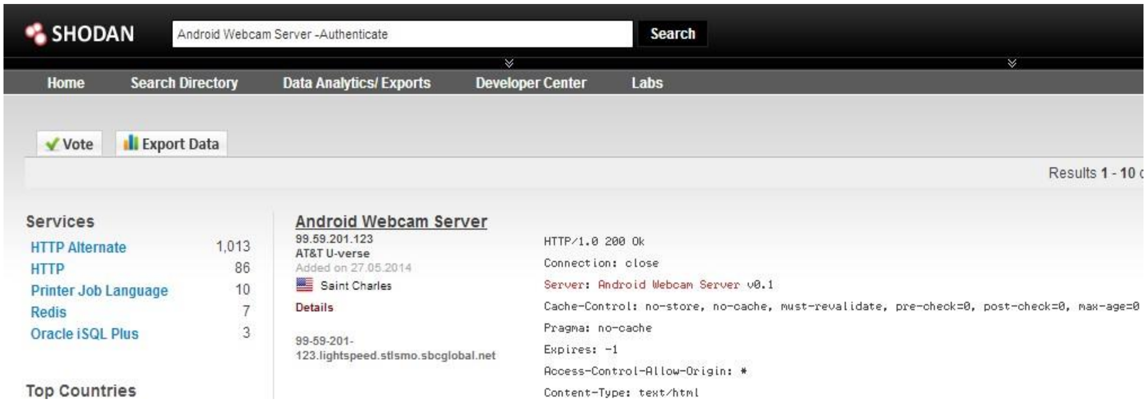
Top Countries	
United Kingdom	45,812
Australia	38,035
Italy	20,341
United States	15,049
Kuwait	8,065

Authorization warning
81.149.30.35
BT
Added on 27.05.2014
London
Details

host81-149-30-35.in-addr.btopenworld.com

```
HTTP/1.0 401 Unauthorized
Server:
Date: Tue, 27 May 2014 06:21:15 GMT
WWW-Authenticate: Basic realm="NETGEAR DG834 "
Content-Type: text/html
Connection: close
```

2)**Webcam:**



Results **1 - 10** c

Services	
HTTP Alternate	1,013
HTTP	86
Printer Job Language	10
Redis	7
Oracle iSQL Plus	3

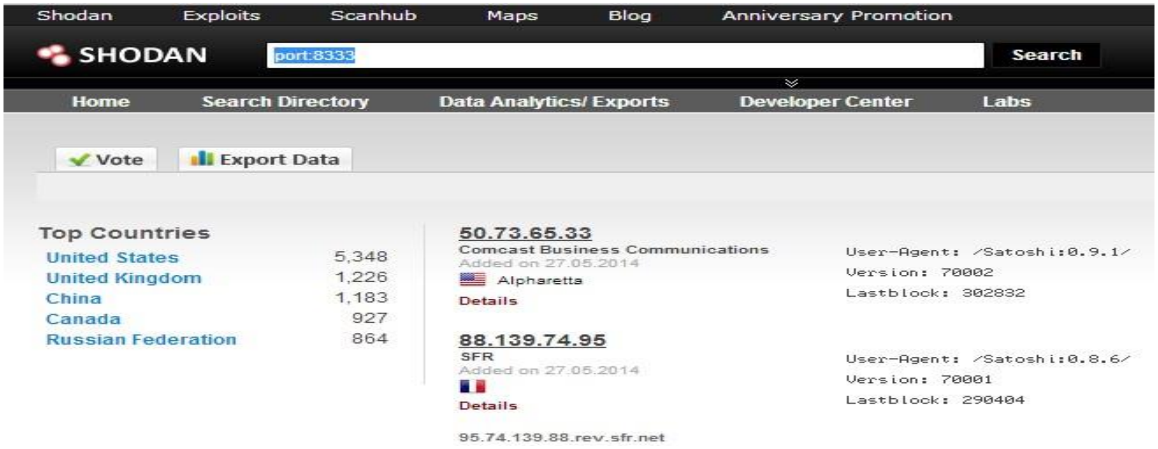
Top Countries

Android Webcam Server
99.59.201.123
AT&T U-verse
Added on 27.05.2014
Saint Charles
Details

99-59-201-123.lightspeed.stlsmo.sbcglobal.net

```
HTTP/1.0 200 Ok
Connection: close
Server: Android Webcam Server v0.1
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Expires: -1
Access-Control-Allow-Origin: *
Content-Type: text/html
```

3)**Bitcoin server:**



Top Countries	
United States	5,348
United Kingdom	1,226
China	1,183
Canada	927
Russian Federation	864

50.73.65.33
Comcast Business Communications
Added on 27.05.2014
Alpharetta
Details

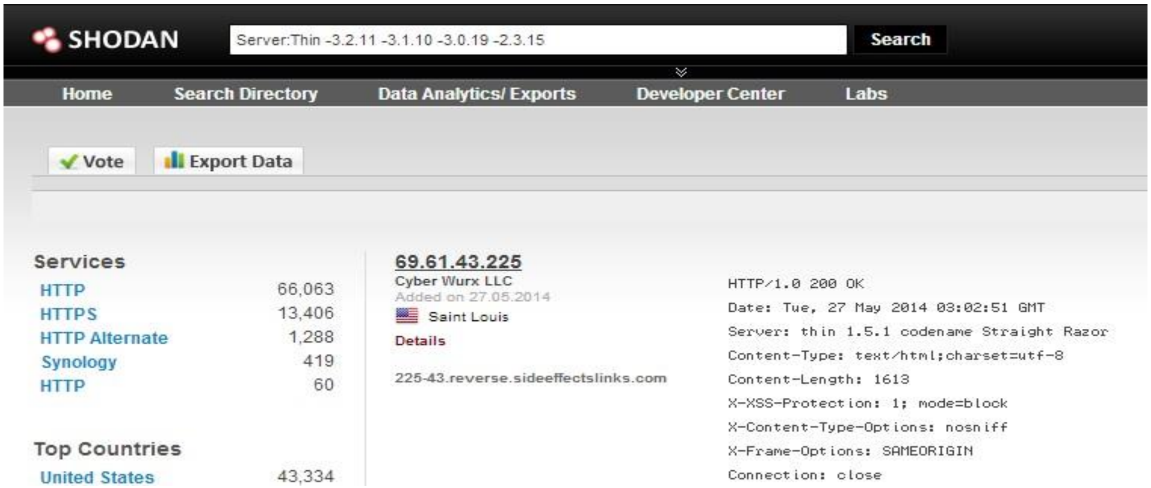
```
User-Agent: /Satoshi:0.9.1/
Version: 70002
Lastblock: 302832
```

88.139.74.95
SFR
Added on 27.05.2014
Details

95.74.139.88.rev.sfr.net

```
User-Agent: /Satoshi:0.8.6/
Version: 70001
Lastblock: 290404
```

4)**Ruby on Rails Vulnerable Server(CVE-2013-0156 and CVE-2013-0155):**



Services	
HTTP	66,063
HTTPS	13,406
HTTP Alternate	1,288
Synology	419
HTTP	60

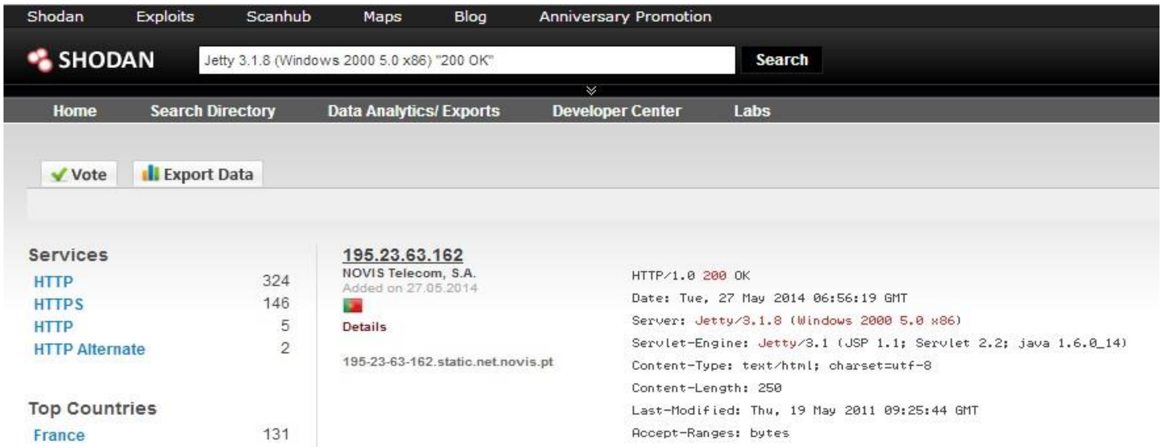
Top Countries	
United States	43,334

69.61.43.225
Cyber Wurx LLC
Added on 27.05.2014
Saint Louis
Details

225-43.reverse.sideeffectslinks.com

```
HTTP/1.0 200 OK
Date: Tue, 27 May 2014 03:02:51 GMT
Server: thin 1.5.1 codename Straight Razor
Content-Type: text/html;charset=utf-8
Content-Length: 1613
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Connection: close
```

5)**Windfarms:**



Services	
HTTP	324
HTTPS	146
HTTP	5
HTTP Alternate	2

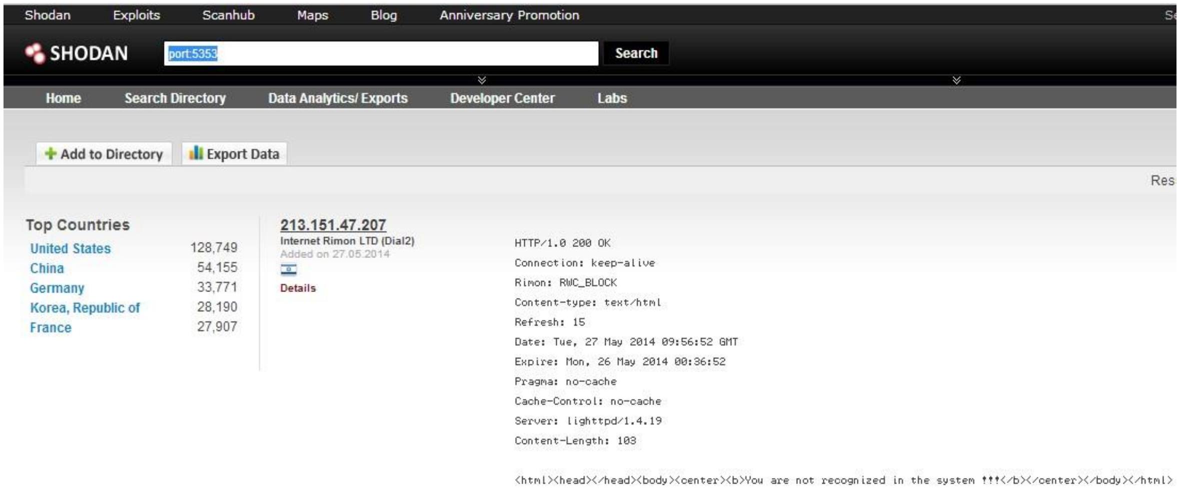
Top Countries	
France	131

195.23.63.162
NOVIS Telecom, S.A.
Added on 27.05.2014
Details

195-23-63-162.static.net.novis.pt

```
HTTP/1.0 200 OK
Date: Tue, 27 May 2014 06:56:19 GMT
Server: Jetty/3.1.8 (Windows 2000 5.0 x86)
Servlet-Engine: Jetty/3.1 (JSP 1.1; Servlet 2.2; java 1.6.0_14)
Content-Type: text/html; charset=utf-8
Content-Length: 250
Last-Modified: Thu, 19 May 2011 09:25:44 GMT
Accept-Ranges: bytes
```

6)**DNS service:**



Top Countries	
United States	128,749
China	54,155
Germany	33,771
Korea, Republic of	28,190
France	27,907

213.151.47.207
Internet Rimon LTD (Dial2)
Added on 27.05.2014
Details

```
HTTP/1.0 200 OK
Connection: keep-alive
Rimon: RWC_BLOCK
Content-type: text/html
Refresh: 15
Date: Tue, 27 May 2014 09:56:52 GMT
Expire: Mon, 26 May 2014 00:36:52
Pragma: no-cache
Cache-Control: no-cache
Server: lighttpd/1.4.19
Content-Length: 103

<html><head></head><body><center><b>You are not recognized in the system !!!</b></center></body></html>
```

Some additional cheat sheet links:

http://www.Shodanhq.com/?q=bitcoin-mining-proxy (Bitcoin proxy mining)

http://www.Shodanhq.com/search?q=port%3A11 (Systat)

http://www.Shodanhq.com/search?q=port%3A8089+splunkd (Splunk servers on tcp/8089)

http://www.Shodanhq.com/search?q=port%3A17(Search for quote of the day)

http://www.Shodanhq.com/search?q=port%3A123(Ntp monlist)

http://www.Shodanhq.com/search?q=port%3A5632 (Vnc)

http://www.Shodanhq.com/search?q=port%3A1434 ((MS-SQL (1434))

http://www.Shodanhq.com/search?q=OpenSSL%2F1.0.1 (Servers running OpenSSL/1.0.1)

http://www.Shodanhq.com/search?q=port%3A79 (Finger protocol)

http://www.Shodanhq.com/search?q=port%3A15 (Netstat)

http://www.Shodanhq.com/?q=telemetry+gateway (Telemetry gateway)

http://www.Shodanhq.com/?q=port:161+country:US+simatic (Simatic automation system on port 161 running in US)

References:

http://www.Shodanhq.com/ https://Shodanio.wordpress.com/

http://www.rapid7.com/db/modules/auxiliary/gather/Shodan_search

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/gather/Shodan_search.rb

http://www.slideshare.net/theprez98/Shodan-for-penetration-testers-defcon-18