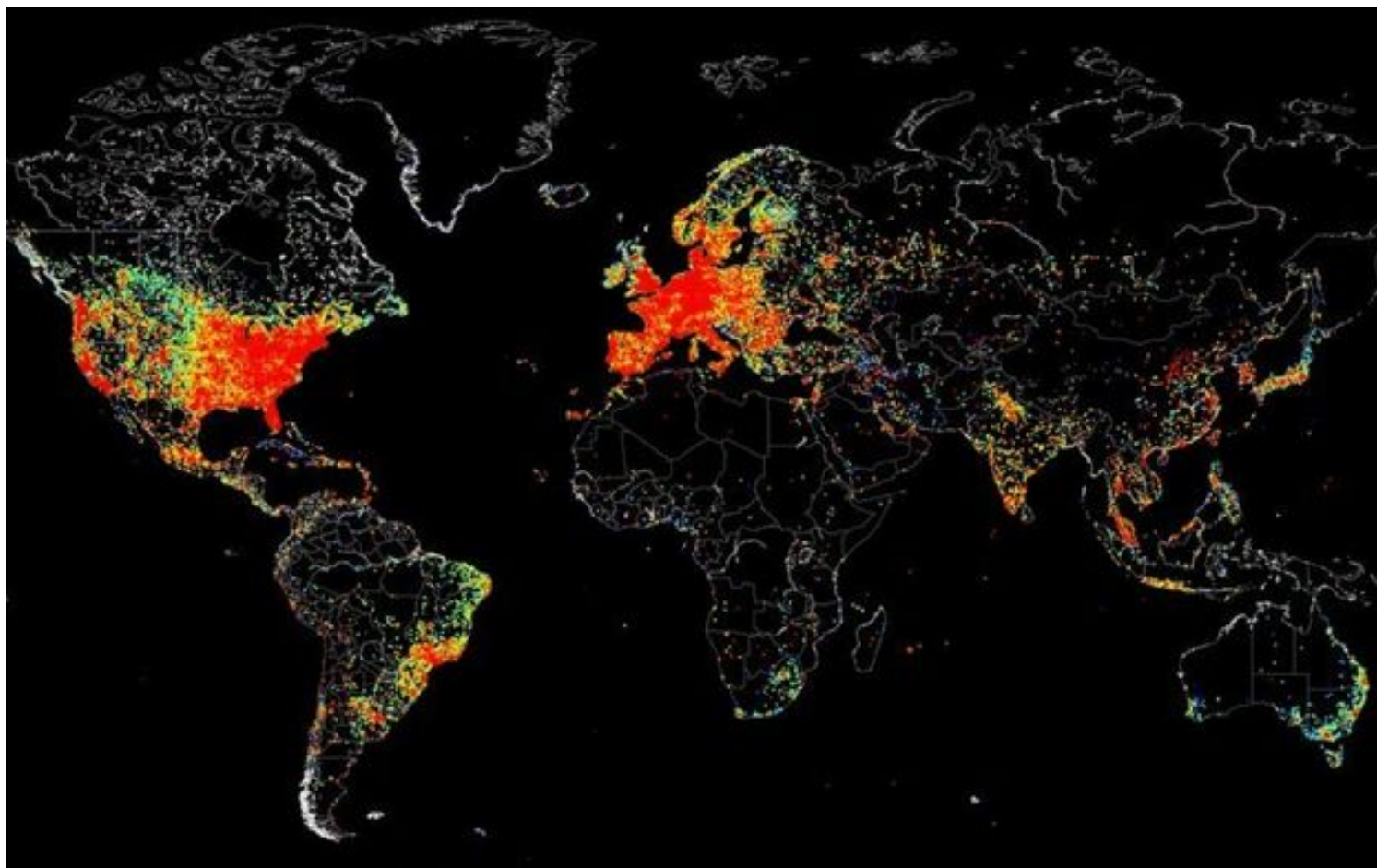


Guide (v1.0) : Shodan

Introduction à Shodan : Collecte, analyse et Développement ...



Kondah Hamza

MVP Sécurité des entreprise
Formateur Alphorm

Alphorm
com



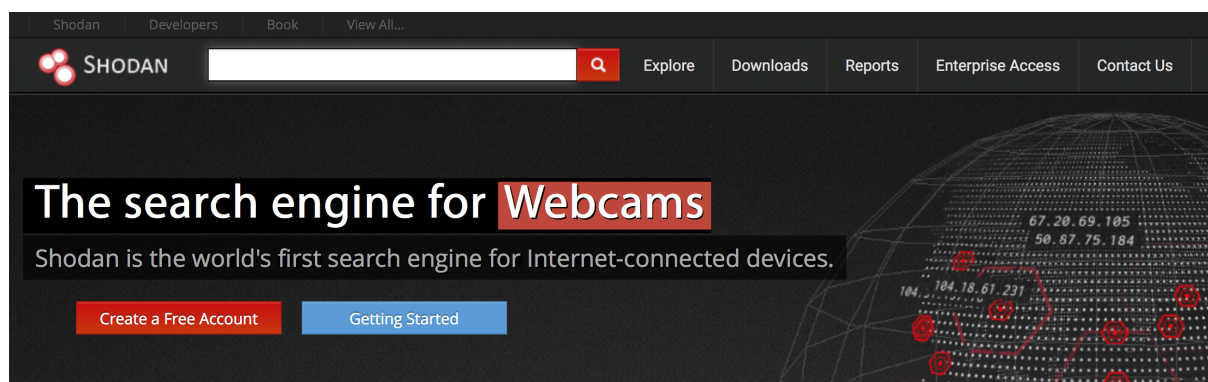
Table des matières

Introduction	3
Comment Shodan arrive-il à tous répertorier ?	4
La récolte d'informations	5
Méthodologie de recherche sur l'interface web de Shodan	6
Reporting.....	10
Shodan Exploit.....	13
Ligne de commande	14
Maltego & Shodan	18
Plugin Navigateur web	19
Api développeur	20
Conclusion	23

Introduction

Shodan (www.shodan.io) est un moteur de recherche (Similaire aux moteurs de recherches traditionnelles tel que **Bing** ou encore **Google**) qui répertorie tous type de périphériques connectés (en IPv4 et IPv6) sur Internet.

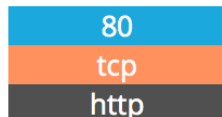
Ce qui est encore plus intéressant avec le moteur de recherche Shodan, c'est qu'il permet de rechercher une machine spécifique à travers des filtres très sophistiqués. Par exemple, une machine faisant tourner un service spécifique, vulnérable à une faille donnée ou encore de récupérer des statistiques relatives à un contexte prédéfini (Os, Version de service, Emplacement etc...).



Comment Shodan arrive-t-il à tous répertorier ?

Afin de pouvoir alimenter sa base de données, Shodan se base tout simplement sur les **bannières**.

Une bannière est une information textuelle décrivant le service qui tourne au sein d'une machine spécifique (Qui varie selon le contexte).



nginx

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 23 May 2017 14:07:31 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.29
Vary: Host,Accept-Encoding
Cache-Control: max-age=0
Expires: Tue, 23 May 2017 14:07:31 GMT
X-Powered-By: PleskLin
```

C'est aussi une information qu'on peut récupérer grâce à une application de scanning tel que NMAP ou encore NESSUS.

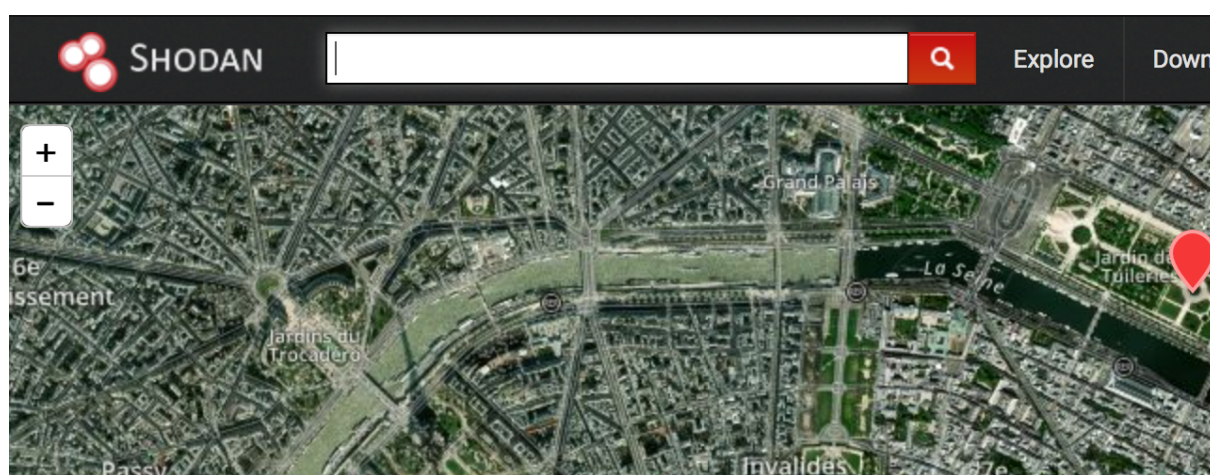
```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-25 15:13 WET
Nmap scan report for cloud.linge-ma.ws (188.241.146.182)
Host is up (0.15s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.10.3 (Ubuntu)
443/tcp   open  ssl/http nginx 1.10.3 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.62 seconds
root@kali:~#
```


La récolte d'informations

Les informations qui sont récupérées ne sont pas seulement relatives aux bannières, mais la récolte se fait aussi au niveau des métas donnés de la machine : Emplacement, nom d'hôte, Os etc...

Ce qui est encore plus intéressant, et ce qu'on va découvrir un peu plus tard dans cet ebook, c'est le fait que Shodan met à disposition aux développeurs une API très simple et extrêmement facile à manipuler 😊 .



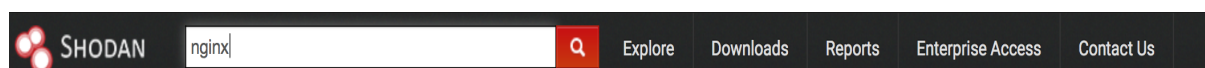
 **62.210.49.129** mail34.ristrettomedia.mxea5.com

Database

City	Paris
Country	France
Organization	ONLINE SAS
ISP	Free SAS
Last Update	2017-05-31T01:17:29.710624
Hostnames	mail34.ristrettomedia.mxea5.com
ASN	AS12876

Méthodologie de recherche sur l'interface web de Shodan

La manière la plus facile et efficace d'exploiter le moteur de recherche Shodan n'est autre qu'à travers son interface web. Par défaut, on retrouve le modèle de résultat suivant :



Le résultat affiche seulement la bannière relative à la machine et non pas les meta données.

Le résultat de recherche est donc relatif à toutes les machines contenant au niveau de la bannière le texte saisi au niveau de la recherche (dans le cas ci-dessous nginx) :

129.121.203.48

drrockso.seoboxes.com

Nexcess.net L.L.C.

Added on 2017-05-31 01:23:12 GMT

 United States, Austin

Details

HTTP/1.1 200 OK

Server: **nginx**

Date: Wed, 31 May 2017 00:55:43 GMT

Content-Type: text/html

Content-Length: 111

Connection: keep-alive

Keep-Alive: timeout=15

Last-Modified: Fri, 11 Nov 2016 19:29:07 GMT

ngpass_ngall: 1

Accept-Ranges: bytes

En cliquant sur **Details** au niveau d'une des machines résultantes suite à la recherche on peut afficher plus de détails sur cette dernière ; Services, ports ouverts, méta données etc...

Ports

22	26	53	80	110	143	443	465	587
993	995	2082	2083	2087	3306	8080		

143
tcp
imap

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAME
SPACE STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
* CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE
STARTTLS AUTH=PLAIN AUTH=LOGIN
A001 OK Pre-login capabilities listed, post-login capabilities have more.
* ID ("name" "Dovecot")
A002 OK ID completed.
A003 BAD Error in IMAP command received by server.
* BYE Logging out
A004 OK Logout completed.
```

443
tcp
https



Apache httpd

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 31 May 2017 00:34:02 GMT
Server: Apache
Location: http://129.121.203.48/
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1
```

SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

36:ee:f0:67:37:1a:d0:e8:a4:69:e4:1f:a3:de:25:85

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN

=COMODO RSA Domain Validation Secure Server CA

On peut affiner les recherches selon plusieurs critères : Ville, Pays, port etc...

La liste des filtres disponibles est la suivante :

Name	Description	Type
after	Only show results after the given date (dd/mm/yyyy)	string
asn	Autonomous system number	string
before	Only show results before the given date (dd/mm/yyyy)	string
category	Available categories: ics, malware	string
city	Name of the city	string
country	2-letter country code	string
geo	Accepts between 2 and 4 parameters. If 2 parameters: latitude,longitude. If 3 parameters: latitude,longitude,range. If 4 parameters: top left latitude, top left longitude, bottom right latitude, bottom right longitude.	string
hash	Hash of the data property	integer
has_ipv6	True/ False	boolean
has_screenshot	True/ False	boolean
hostname	Full hostname for the device	string
ip	Alias for net filter	string
isp	ISP managing the netblock	string
net	Network range in CIDR notation (ex. 199.4.1.0/24)	string
org	Organization assigned the netblock	string
os	Operating system	string
port	Port number for the service	integer
postal	Postal code (US-only)	string
product	Name of the software/ product providing the banner	string
region	Name of the region/ state	string
state	Alias for region	string
version	Version for the product	string
vuln	CVE ID for a vulnerability	string

Les filtres peuvent être utilisés de la manière suivante :

NomDuFiltre :Valeur

Quelques exemples d'utilisation de filtre :

- Par ville : city:"Paris"

SHODAN city:"paris" [Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#) [My Account](#) [Upgrade](#)

[Exploits](#) [Maps](#) [Images](#) [Share Search](#) [Download Results](#) [Create Report](#)

TOTAL RESULTS
526,265

TOP COUNTRIES



France	517,891
United States	7,429
Canada	945

TOP SERVICES

HTTP	80,645
HTTPS	52,961
SSH	40,542
HTTP (8080)	20,403

62.210.49.129
mail34.netrettomedia.mwea5.com
ONLINE SAS
Added on 2017-05-31 01:17:29 GMT
France, Paris
[Details](#)

* OK IMAP4rev1 Server Ready.
* CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE AUTH=LOGIN AUTH=PLAIN AUTH=CRAM-MD5 AUTH=CRAM-SHA1 AUTH=CRAM-SHA256 STARTTLS XCOURIEROUTBOX=INBOX.Outbox
A001 OK CAPABILITY completed
A002 NO Error in IMAP comm...

176.183.74.129
static-176-183-74-129.ncc.abo.bbox.fr
Bouygues Telecom
Added on 2017-05-31 01:17:25 GMT
France, Paris
[Details](#)

RTSP/1.0 200 OK
CSeq: 1
Date: Wed, 31 May 2017 00:49:55 GMT
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY

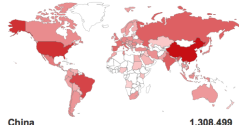
- Par port : port:23,1023

SHODAN port:23,1023 [Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#) [My Account](#) [Upgrade](#)

[Exploits](#) [Maps](#) [Images](#) [Share Search](#) [Download Results](#) [Create Report](#)

TOTAL RESULTS
5,928,068

TOP COUNTRIES



China	1,308,499
United States	694,296
Brazil	433,601
Korea, Republic of	290,199
India	245,742

TOP SERVICES

Telnet	5,909,084
Telnet (1023)	18,984

TOP ORGANIZATIONS

Korea Telecom	154,685
Orange	107,308
BSNL	98,610
Telefonica de Espana	94,023
Vivo	62,157

110.83.28.125
125.28.83.110.broad.fz.dynamic.163data.com.cn
China Telecom fujian
Added on 2017-05-31 01:28:49 GMT
China, Fuzhou
[Details](#)

* Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowe... *

92.115.75.63
host-static-92-115-75-63.moldtelecom.md
JSC Moldtelecom S.A.
Added on 2017-05-31 01:28:49 GMT
Moldova, Republic of
[Details](#)

User:

216.155.93.248
Telefonica del Sur S.A.
Added on 2017-05-31 01:28:46 GMT
Chile, Valdivia
[Details](#)

User Access Verification

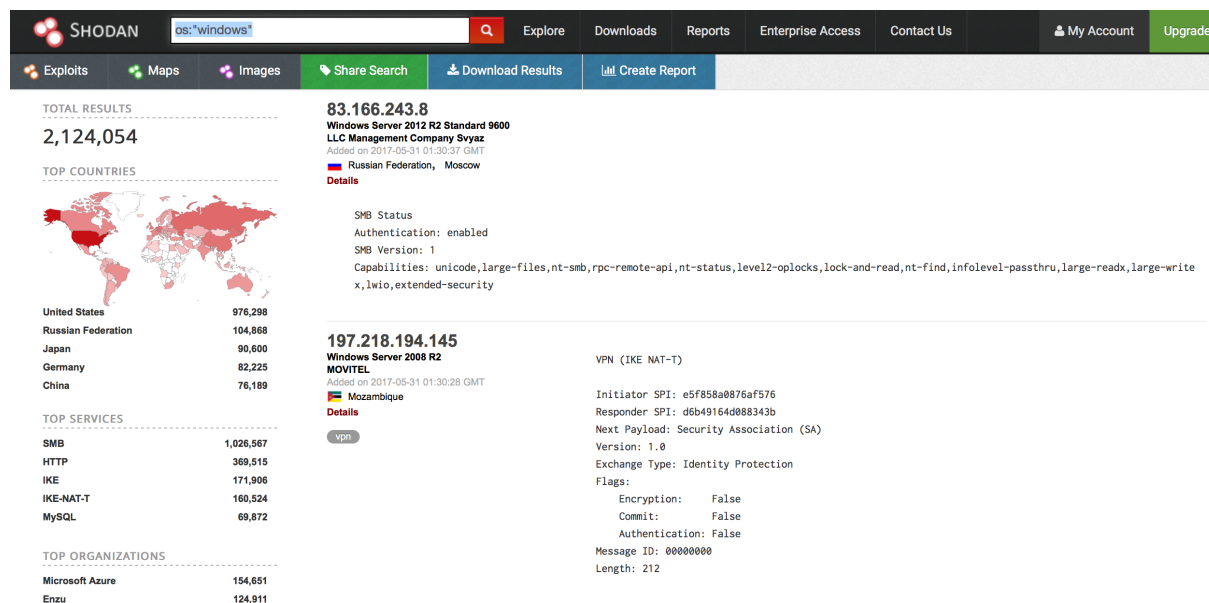
Password:

119.52.249.146
146.249.52.119.adsl-pool.jccptt.net.cn
China Unicom Jilin
Added on 2017-05-31 01:28:46 GMT
China, Changchun
[Details](#)

Welcome to ZXRI0 Carrier-class High-end Routing Switch of ZTE Corporation

Username:

- Par système d'exploitation : os : "Windows"



Reporting

Shodan permet aussi de pouvoir générer des rapports extrêmement détaillés, contenant des graphs et des statistiques très intéressantes. Vous pouvez générer des rapports relatifs à une recherche (des filtres)

en appuyant sur le bouton [Create Report](#)

Le résultat ressemble à l'exemple suivant :

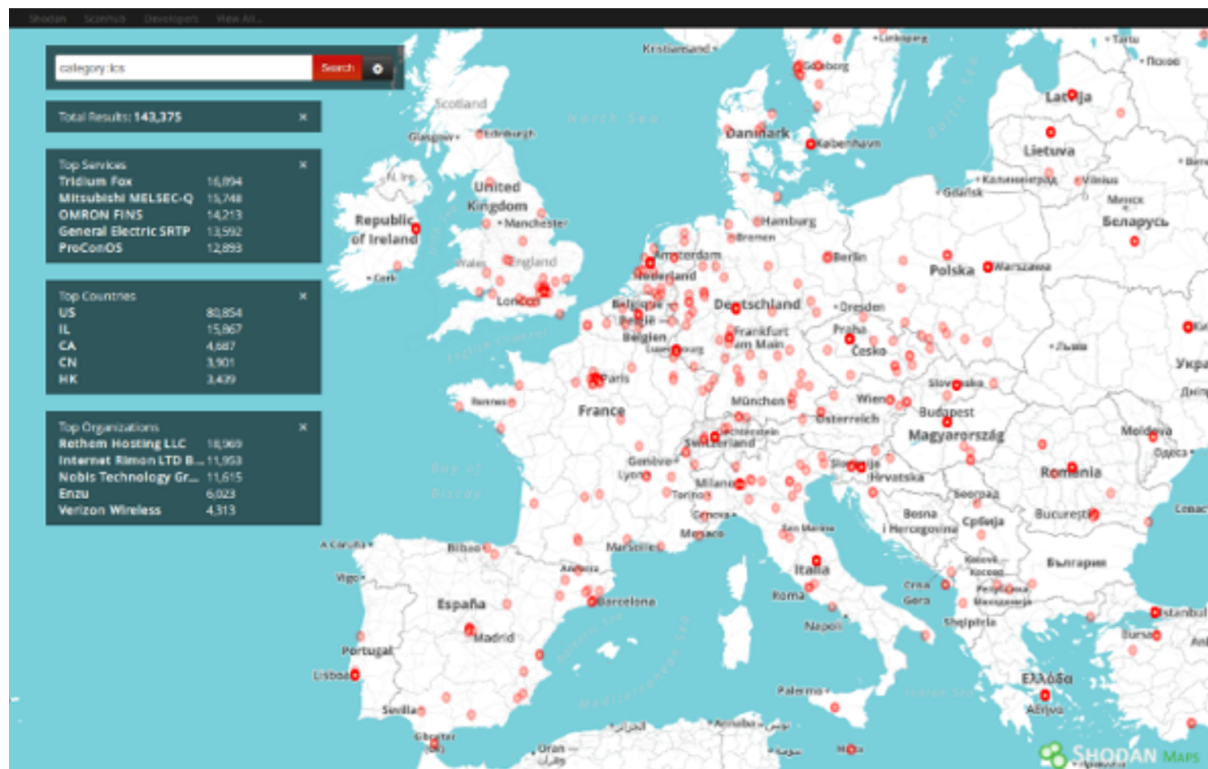


Shodan nous permet aussi de pouvoir afficher le résultat des recherches sur une map détaillée sous différents formats comme on peut le remarquer ci-dessous :

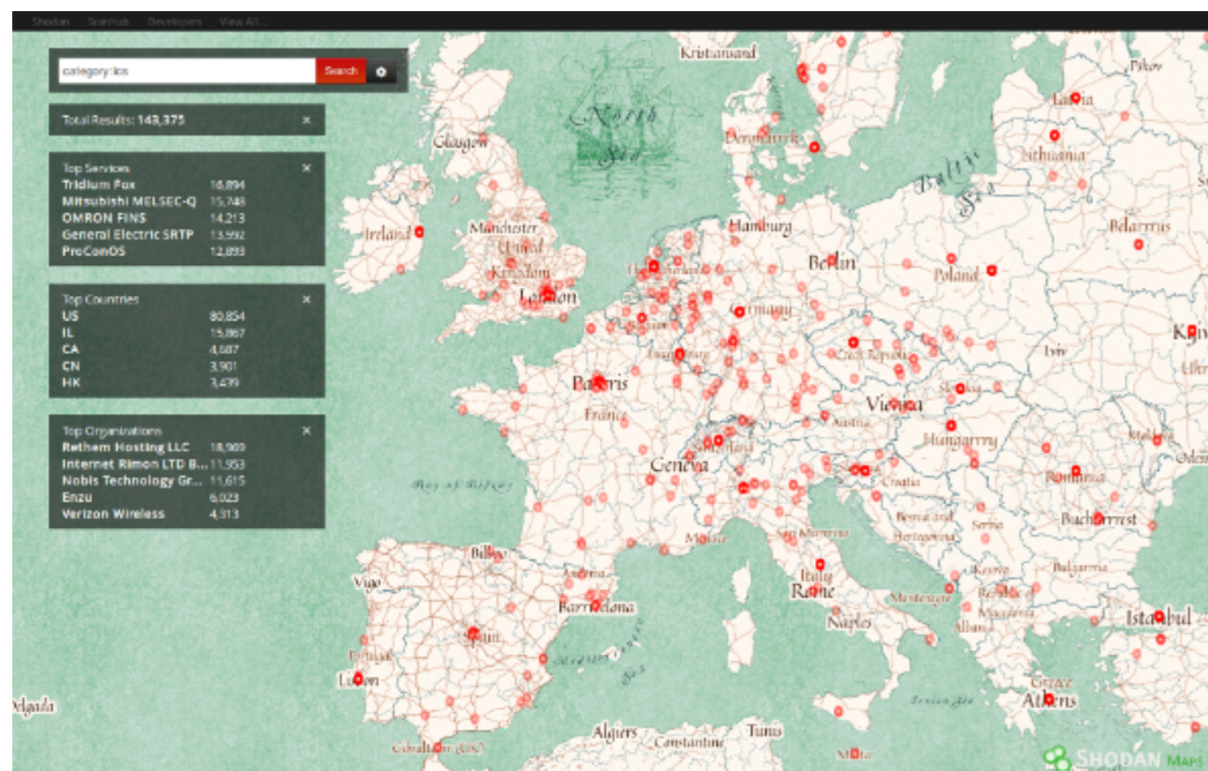
- **Satellite :**



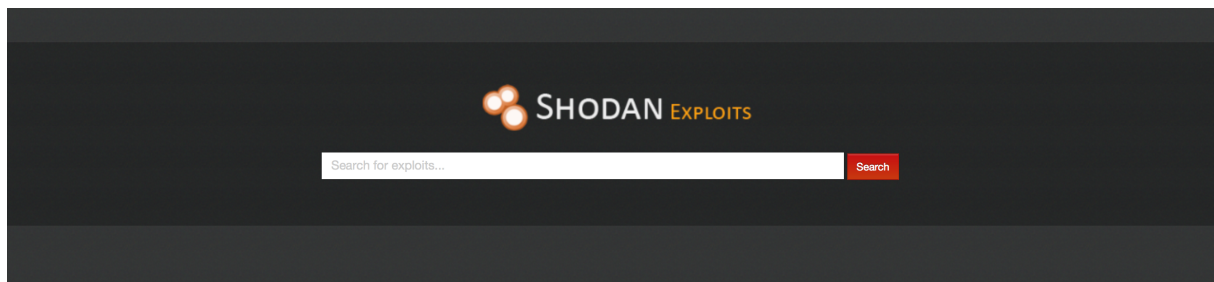
- **Street :**



- **Pirate :**

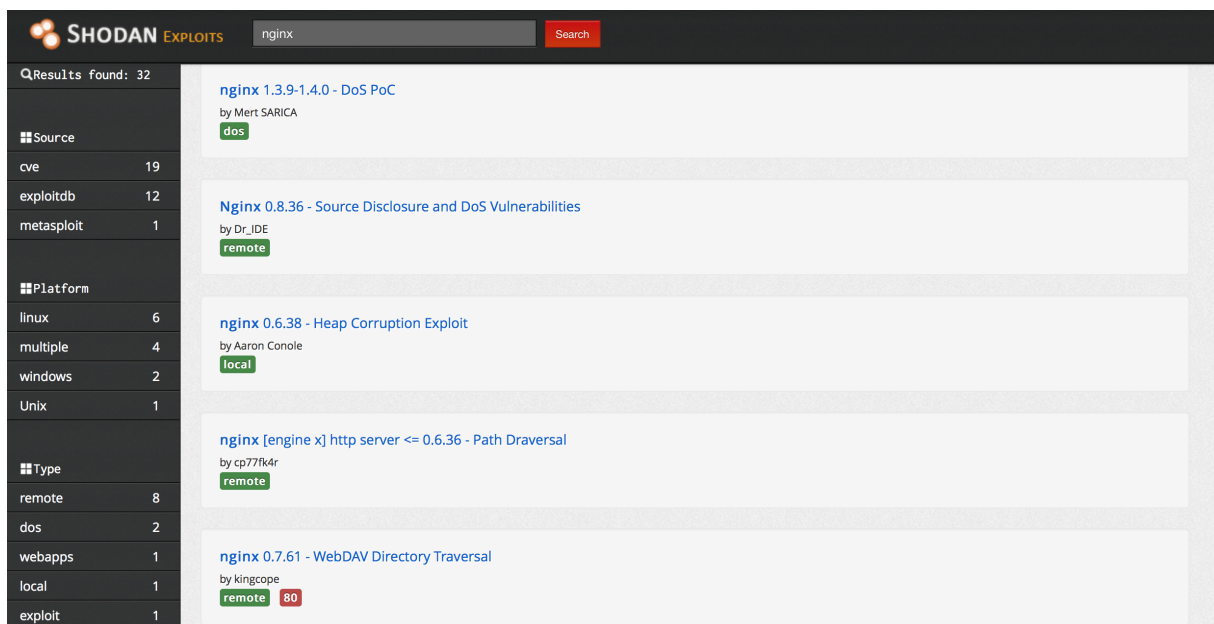


Shodan Exploit



Le module exploit de shodan répertorie tous les exploits présents dans les bases e données suivantes :

- **CVE**
- **Exploit DB**
- **Metasploit**



Les filtres disponibles sont les suivants :

Name	Description
Author	Author of the vulnerability / exploit
Description	Description
Platform	Platform that it targets (ex : php , windows , linux)
Type	Exploit type (ex : remote , dos)

Ligne de commande

Shodan est aussi disponible en ligne de commande.

Vous pouvez installer le paquet shodan en utilisant la commande suivante :

“Easy_install shodan”

Ensuite il vous faudra initialiser shodan grâce à la clé API que vous pouvez récupérer sur votre compte grâce à la commande suivante :

Shodan init API_KEY

```
root@kali:~# shodan init otj3Ez3MkyIK8pAWetPbHBgRgXZ15FIo
Successfully initialized
root@kali:~#
```

À partir de là, vous pouvez afficher la liste des commandes disponibles grâce à la commande suivante :

```

root@kali:~# shodan -h
Usage: shodan [OPTIONS] COMMAND [ARGS]...

Options:
  -h, --help  Show this message and exit.

Commands:
  alert      Manage the network alerts for your account
  convert    Convert the given input data file into a...
  count      Returns the number of results for a search
  download   Download search results and save them in a...
  honeyscore Check whether the IP is a honeypot or not.
  host       View all available information for an IP...
  info       Shows general information about your account
  init       Initialize the Shodan command-line
  myip       Print your external IP address
  parse      Extract information out of compressed JSON...
  scan       Scan an IP/ netblock using Shodan.
  search     Search the Shodan database
  stats      Provide summary information about a search...
  stream     Stream data in real-time.
root@kali:~#

```

Ci-dessous quelques exemples d'utilisation :

Afficher le nombre de machines relatives à une recherche spécifique :

```

root@kali:~# shodan count microsoft iis 6.0
502232
root@kali:~#

```

Télécharger le résultat d'une recherche :

```

root@kali:~# shodan download microsoft-data microsoft iis 6
Search query:      microsoft iis 6
Total number of results: 7005
Query credits left: 0
Output file:       microsoft-data.json.gz
[#####] 100%
Notice: fewer results were saved than requested
Saved 100 results into file microsoft-data.json.gz
root@kali:~#

```

Recherche spécifique à un hôte :


```

root@kali:~# shodan host 39.108.3.29
39.108.3.29
City: Hangzhou
Country: China
Organization: Aliyun Computing Co.
Number of open ports: 2

Ports:
  80 nginx
 3306 MySQL (5.6.36-log)
root@kali:~#

```

Vérifier l'existence d'un honeypot :

```

root@kali:~# shodan honeyscore 39.108.3.29
Not a honeypot
Score: 0.0
root@kali:~#

```

Récupération de statistiques :

```

root@kali:~# shodan stats --facets country apache
Top 10 Results for Facet: country
US challenge 7,414,100
MX 3,133,834
DE 1,612,901
JP 1,434,370
CN 1,033,583
FR Challenge. 836,380
GB png 706,900
NL 579,567
CA 493,056
RU 440,777
root@kali:~#

```

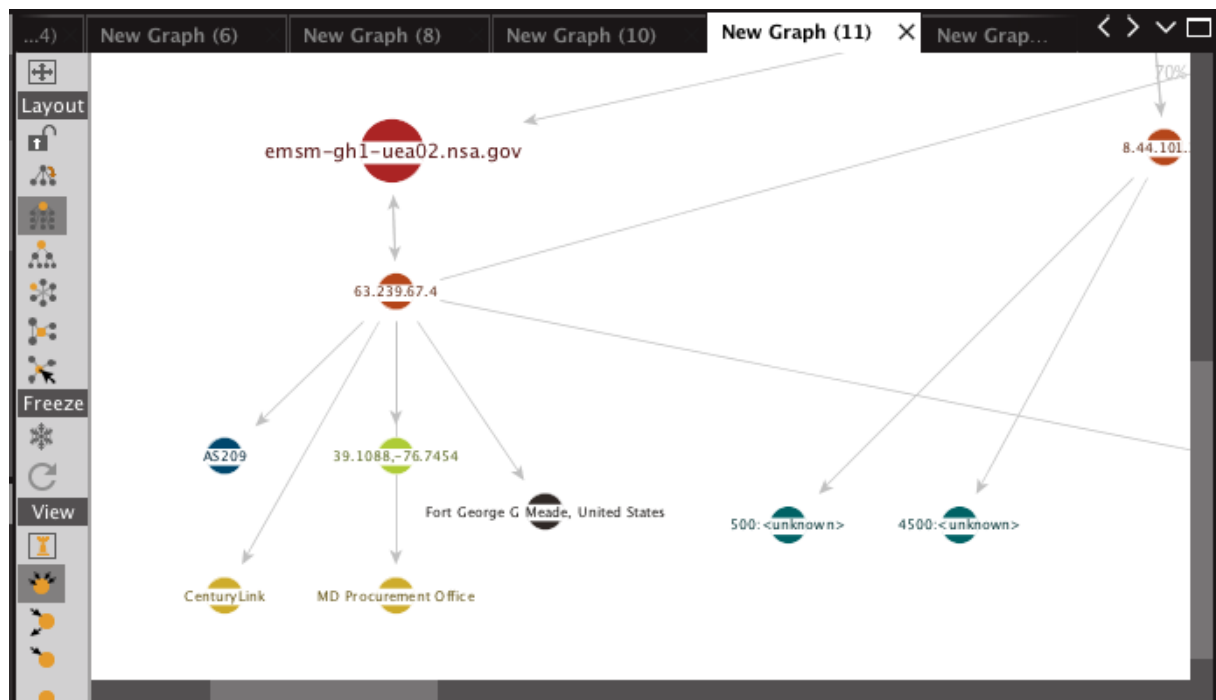
Spécifier les champs à afficher :

```
root@kali:~# shodan search --fields ip_str,port,org,hostnames microsoft iis 6.0
```

223.6.205.209	80	Hangzhou Alibaba Advertising Co.,Ltd.
174.136.147.214	80	Web Elite LLC
223.6.27.219	80	Hangzhou Alibaba Advertising Co.,Ltd.
107.149.22.58	80	Peg Tech
45.61.242.139	80	Hostspace Networks LLC
66.222.36.196	80	TDS Telecom h66-222-36-196.nlsnga.broadband.dynamic.tds.net
104.216.158.5	80	Psychz Networks
204.168.72.38	80	ClearBlue Technologies
108.187.111.79	80	SpeedVM Network Group LLC
202.14.70.64	80	PIA www.piac.aero
61.219.107.208	82	HiNet www.good-men.com
59.153.145.136	80	Heng Tong
202.119.85.153	8080	Nanjing University of Science & Technology
177.53.151.21	80	Itmnetworks Ltda 177-53-151-21.itmnetworks.net.br
64.136.158.138	8080	Aerioconnect mail.ericadler.com
23.80.192.142	80	Nobis Technology Group, LLC
194.12.13.54	80	C.C.S. (Leeds) Ltd 194-12-13-54.ccsleeds.co.uk
122.9.232.82	80	HKDF
216.119.85.227	80	CrystalTech Web Hosting
50.194.135.77	80	Comcast Business 50-194-135-77-static.hfc.comcastbusiness
80.247.1.187	80	Net Energy Internet Ltd. www.davieconstruction.co.uk
113.207.121.135	80	China Unicom Chongqing
47.88.106.74	80	Alibaba
187.72.13.34	80	Algar Telecom S/a isa2.eptv.com.br
107.160.28.165	80	Psychz Networks
103.225.199.165	80	Gigabit Hosting Sdn Bhd
107.151.65.183	80	Sun Network (Hong Kong) Limited - HongKong Backbon

Maltego & Shodan

Il est possible d'exploiter Shodan sur Maltego, extrêmement utile dans la phase de reconnaissance et forensics à travers le module existant sous ce dernier :

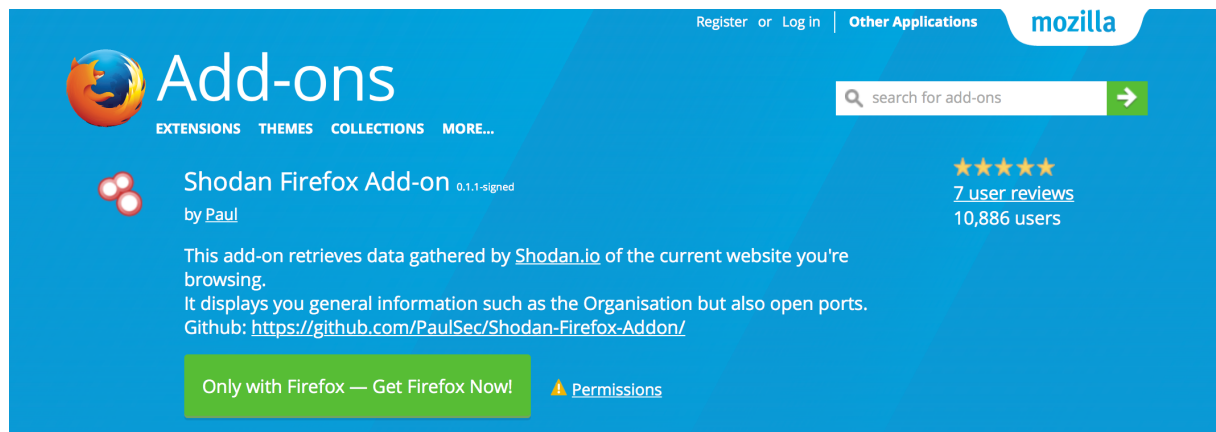


Les transformations disponibles sont les suivantes :

- **Searchshodan**
- **Searchshodanbydomain**
- **Searchshodanbynetblock**
- **Toshodanhost**
- **Searchexploits**

Plugin Navigateur web

Il existe un plugin Shodan pour les navigateurs Chrome et Firefox qui vous permettent de récupérer la liste des services exposés relatif à un serveur web



Api développeur

On arrive à la partie la plus intéressante, qui est l'api de développement de SHODAN.

Shodan fournit une api pour les développeurs (**<https://developer.shodan.io>**) afin de pouvoir coder vos applications personnalisées en exploitant la base de données de Shodan.

[illegible]

L'API se compose de deux parties : REST API and Streaming API.

L'api REST fournit les méthodes de recherche sur Shodan, recherche d'un hôte, informations détaillées, requêtes personnalisées ainsi que d'autres méthodes permettant de faciliter le développement.

L'API streaming fournit quant à elle des résultats en raw, flux en temps réel et les différentes informations collectées par shodan.

Afin de pouvoir utiliser l'API de Shodan (En Python), nous allons tout d'abord initialisation l'objet api de shodan :

```
import shodan api = shodan.Shodan('API KEY')
```


Ci-dessous, nous retrouvons quelques exemples de manipulation à effectuer grâce à l'API de Shodan :

try:

```
# Search Shodan  
results = api.search(nginx)  
# Show the results  
print 'Results found: %s' % results['total']  
for result in results['matches']:  
    print 'IP: %s' % result['ip_str']  
    print result['data']  
    print "  
except shodan.APIError, e:  
    print 'Error: %s' % e
```

Recherche relative à une liste d'hôtes :

```
scan = api.scan('198.2.61.0/24')  
scan = api.scan(['198.2.4.33', '198.20.74.0/24'])
```

Recherche et récupération d'informations sur un hôte :

```
# Lookup the host  
  
host = api.host('217.140.75.46')  
# Print general info  
print """  
    IP: %s  
    Organization: %s  
    Operating System: %s  
""" % (host['ip_str'], host.get('org', 'n/a'), host.get('os', 'n/a'))  
# Print all banners  
for item in host['data']:  
    print """  
        Port: %s  
        Banner: %s
```

```
""" % (item['port'], item['data'])
```

Création d'alertes relatives à la liste d'hôtes (liste d'adresses IP) :

```
alert = api.create_alert ('Production network',  
'198.20.69.0/24')
```

Vous pouvez trouver toutes les informations relatives à l'exploitation de la librairie de développement Shodan sur le site officiel.

API DOCUMENTATION

Requirements

Introduction

Clients

REST API Documentation

Streaming API Documentation

EXPLOITS API DOCUMENTATION

Introduction

REST API Documentation

APPENDIX

Banner Specification

Exploit Specification

Clients/ Libraries

For some of the popular programming languages there are libraries that make it easy to access the Shodan API.
Want your client listed here? Contact us at support@shodan.io with a link to the documentation/ source code repository.

Python

shodan	Github Repository	@achillean	Official Shodan library for Python
--------	-----------------------------------	----------------------------	------------------------------------

Ruby

shodan	Github Repository	@achillean	Official Shodan library for Ruby
--------	-----------------------------------	----------------------------	----------------------------------

PHP

Shodan-PHP-REST-API	Github Repository	@ISGroupSRL	Lean and easily extendible PHP API for Shodan.io, supporting both the free API and the paid one.
---------------------	-----------------------------------	-----------------------------	--

C#

Shodan.Net	Github Repository	@TerribleDev	A C# API client that supports all of the REST API. Streaming API support is still in-progress.
------------	-----------------------------------	------------------------------	--

Conclusion

Shodan représente une révolution dans le volet des moteurs de recherche orientée cyber sécurité, il a permis et démontré que les informations exposées sur internet peuvent être récupérée d'une facilité déconcertante et donc accessible facilement pour les hackers. Il est très important pour chacun de pouvoir vérifier les informations exposés grâce à ce dernier sur internet (surtout dans le cas d'infrastructure critiques tels que les ICS : Industrial Control systems) Lors des prochaines versions de ce guide, nous allons essayer d'approfondir nos connaissances concernant l'exploitation de Shodan, surtout concernant l'API de ce dernier.