

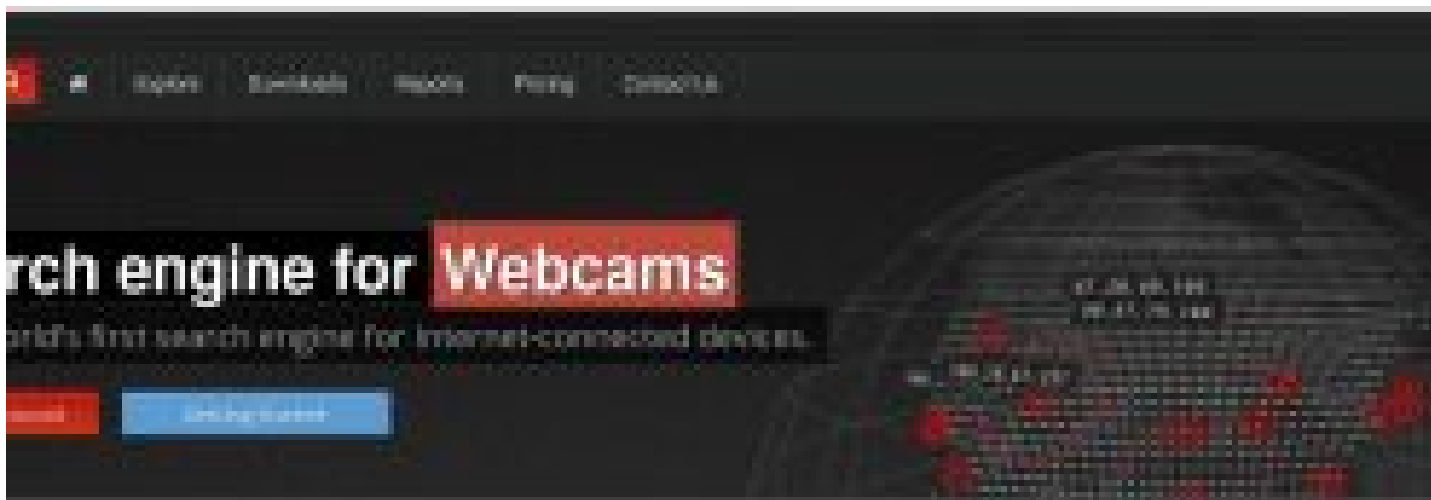


Passive Data Collecting: Shodan



by **Melisa Ayşe Demirel** — 20 April 2019 in **Cyber Security**

0



Explore the Internet of Things

Shodan is designed to discover what your devices are connected to the Internet, & they are located and who is using them.



Monitor Network Security

Thousands of servers, computers on your network that are directly accessible from Internet. Shodan helps you understand your digital footprint.



See the Big Picture

Webcams are just one part of the Internet. There are power refrigerators and machines that can be found with Shodan.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan for competitive intelligence.

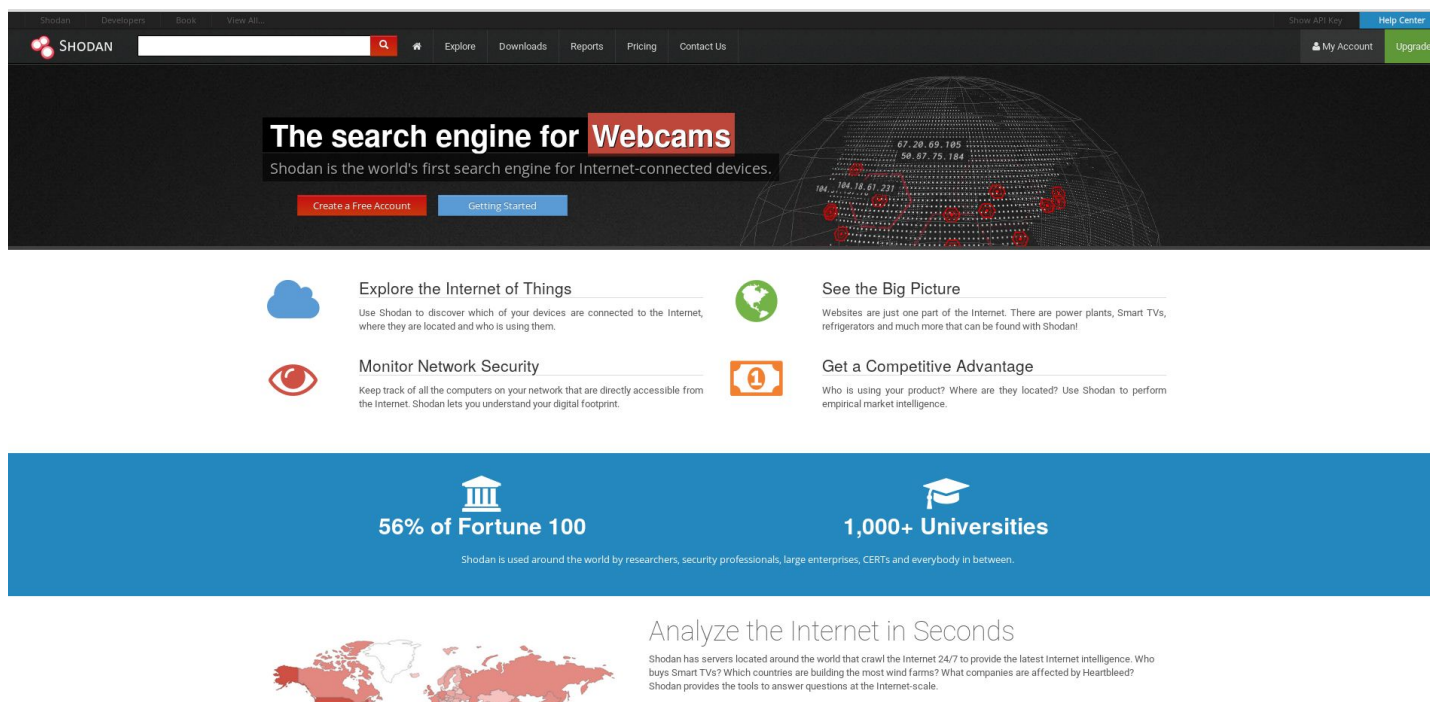


Data collecting is the first step of pentesting. The more data you have, easier and faster it is to be successful. Passive data collecting is collecting data about your target without directly contacting your target. Which means, from the internet. There's lots of tools and methods to collect data about a target though Shodan has always been on the first lines.

Basically, Shodan is almost the same as Google. Though there are some features of Shodan that makes it different than Google. Shodan can scan the internet to see systems, devices and etc. on the internet and classifies them depending on their ports, operating systems, locations and service data. Then uses these informations to scan the possible vulnerabilities. With these informations, you can search based on any country you want. Not only that, with ScanHub service, Shodan can also get the outputs of some scanning devices which helps with analyzing the results visually. (You must pay to get this feature.)

With Shodan, access hidden cameras connected to the internet, SSH servers, web applications, network devices, SCADA and PLC systems and much more.

Sample Image:



There's specific search commands in Shodan, just like Google.

Port Scanning

port:23

SHODAN port:23

Exploits Maps Images Share Search Download Results Create Report

TOTAL RESULTS
5,683,534

TOP COUNTRIES

China	1,329,546
United States	633,388
Russian Federation	356,822
Brazil	347,384
Korea, Republic of	209,965

TOP ORGANIZATIONS

China Telecom Shanghai	155,476
Korea Telecom	143,766
Orange	124,107
Rostelecom	109,283
Globalnet	107,412

TOP OPERATING SYSTEMS

Linux 3.x	4,443
Linux 2.6.x	3,530
Windows 7 or 8	493
Windows XP	253
Linux 2.4.x	92

TOP PRODUCTS

Cisco router telnetd	175,050
OpenSSH	21,703
Cisco catalyst switch telnetd	11,584
Dropbear sshd	3,732
Microsoft Rdp	1,631

113.27.65.20
China Telecom shanghai
Added on 2018-12-02 12:27:27 GMT
China
Details

Welcome Visiting Huawei Home Gateway
Copyright by Huawei Technologies Co., Ltd.
Login:

182.59.170.27
mahana.net.in 182.59.170.27.mahana.net.in
Mahanagar Telephone Nigam
Added on 2018-12-02 12:27:26 GMT
India, Mumbai
Details

175.172.239.172
China Unicom Liaoning
Added on 2018-12-02 12:27:14 GMT
China
Details

216.176.144.17
netnic.net 216.176.144.17.netnic.net
NetNTO
Added on 2018-12-02 12:27:13 GMT
United States, Crown Point
Details

181.111.238.185
Host 181.111.238.185 telecom.net.ar
Telecom Argentina S.A.
Added on 2018-12-02 12:27:04 GMT
Argentina, Catamarca
Details

* All rights reserved (2005-2008) *
* Without the owner's prior written consent, *
* No decompiling or reverse-engineering shall be allowed. *
* Notice: ...

60.16.6.13
China Unicom Liaoning
Added on 2018-12-02 12:27:03 GMT
China
Details

Warning: Telnet is not a secure protocol, and it is recommended to use Sshnet.
Login authentication
Username:

As you can see, it shows us systems with their 23rd (telnet) port open. You don't have to search a specific port all the time, you can search for port intervals too.


port:21-25 and 80

SHODAN port:21-25 and 80

Exploits Maps Share Search Download Results **1** Create Report

TOTAL RESULTS
2,567

TOP COUNTRIES



Country	Count
United States	1,008
Germany	260
Korea, Republic of	164
China	154
France	146

TOP SERVICES

Service	Count
HTTPS	1,179
FTP	528
Oracle	196
HTTP (81)	159
8081	110

TOP ORGANIZATIONS

Organization	Count
A2 Hosting	464
Korea Telecom	150
Amazon.com	124
Hurricane Electric	82
OVH SAS	64

TOP OPERATING SYSTEMS

OS	Count
Linux 3.x	23
Windows 7 or 8	3
Linux 2.6.x	3

TOP PRODUCTS

Product	Count
Apache httpd	1,391
Pure-FTPd	528
NetSupport PC remote control	160
Redis key-value store	34

104.236.95.194
aprilavip.com
Digital Ocean
Added on: 2018-12-02 12:34:30 GMT
United States, New York
[Details](#)

HTTP/1.1 200 OK
Date: Sun, 02 Dec 2018 12:34:30 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1335
Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index ...
```

192.99.250.195
OVH Hosting
Added on: 2018-12-02 12:31:48 GMT
Canada, Montréal
[Details](#)

SSL Certificate
Issued By: 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
Issued To: 220-You are user number 1 of 80 allowed.
Issued To: 220-Local time is now 07:25. Server port: 21.
Issued To: 220-This is a private system ~ No anonymous login
Issued To: 220-[IPv6 connections are also welcome on this server.
Issued To: 220 You will be disconnected after 20 minute...

Supported SSL Versions
TLSv1.1, TLSv1.2

68.66.244.204
68.66.244.204.static.supertcp.com
A2 Hosting
Added on: 2018-12-02 12:25:29 GMT
United States, Ann Arbor
[Details](#)

SSL Certificate
Issued By: 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
Issued To: 220-You are user number 3 of 80 allowed.
Issued To: 220-Local time is now 13:25. Server port: 21.
Issued To: 220-This is a private system ~ No anonymous login
Issued To: 220-IPv6 connections are also welcome on this server.
Issued To: 220 You will be disconnected after 15 minute...

Supported SSL Versions
TLSv1.1, TLSv1.2

5.45.112.26
Fastps Eestli Ou
Added on: 2018-12-02 12:34:30 GMT

Now we searched between 21-25 port intervals and 80th port. To see more details, click the “**Details**” button below the IP address.

Shodan

Developers

Book

View All...

SHODAN

Explore

Downloads

Reports

Pricing

Contact Us

Show

104.236.95.194

aeralawnpro.com

View Raw Data

cloud

starttls

Database

City	New York
Country	United States
Organization	Digital Ocean
ISP	Digital Ocean
Last Update	2018-12-02T12:34:30.549975
Hostnames	aeralawnpro.com
ASN	AS14061

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-0117	The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.
CVE-2014-0118	The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.
CVE-2016-0736	In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

Ports

21

22

25

53

80

110

123

143

443

465

587

993

995

8081

Services

21

ftp

Pure-FTPD

220----- Welcome to Pure-FTPd [privsep] [TLS] -----

220-You are user number 1 of 50 allowed.

220-Local time is now 11:18. Server port: 21.

220-This is a private system - No anonymous login

220-IPv6 connections are also welcome on this server.

220 You will be disconnected after 15 minutes of inactivity.

530 Login authentication failed

214-The following SITE commands are recognized

ALIAS

CHMOD

IDLE

UTIME

214 Pure-FTPd - http://pureftpd.org/

211-Extensions supported:

EPRT

IDLE

MODT

On the map above, you can see your target's location. On the right side, you can see open port that their system have. It shows currently working services on the system, right below it. Wait a minute, it also shows the vulnerabilities on the left side! 😊 Like I said earlier, Shodan does port, service and vulnerability scanning. That's the exact reason why it's such an important tool. You can get into the system by exploiting. By the way, you can also search exploits on Shodan.

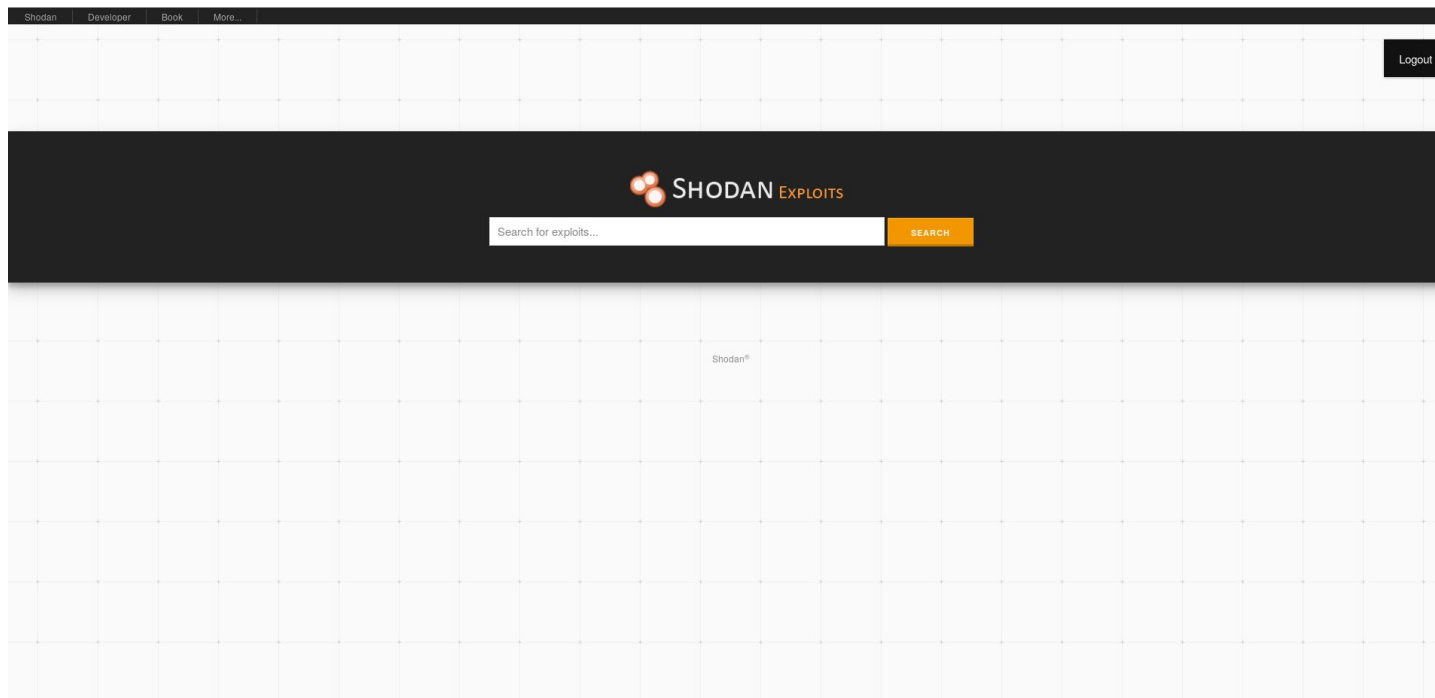
Filter	Command	Example
Author	author	author:"kingcope"
Bugtraq ID	bid	bid:"48581"
Exploit Code	code	code:"</D:propfind>"

Create PDF in your applications with the Pdfcrowd [HTML to PDF API](#)

PDFCROWD

CVE	cve	cve:"CVE-2011-2064"
Exploit Description	description	description:"cisco content"
Microsoft Security Bulletin ID	msb	msb:"MS16-010"
Open Source Vulnerability DB ID	osvdb	osvdb:"86562"
Source	source	source:"CVE"
Platform	platform	platform:"linux"
Port	port	port:"443"
Title	title	title:"Apache Win32"
Type	type	type:"remote"

link: exploits.shodan.io



Exploit Scanning

author:ismail tasdelen

Shodan Developer Book More

SHODAN Exploits author:ismail tasdelen

Logout

TOTAL RESULTS
24

PLATFORM

php	9
hardware	9
ruby	2
java	2
windows_x86-64	1

LANGO Codeigniter Multilingual Script 1.0 - Cross-Site Scripting
ismail Tasdelen
webapps

```
... # Exploit Title: LANGO Codeigniter Multilingual Script 1.0 - Cross-Site Scripting
# Date: 2018-10-16
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: http://pokkho.com/lango/
# Software Link : http://pokkho.com/lango/auth/login
# Software : LANGO - Codeigniter Multilingual Script ...
```

LANGO Codeigniter Multilingual Script 1.0 - Cross-Site Scripting
ismail Tasdelen
webapps

```
... # Exploit Title: LANGO Codeigniter Multilingual Script 1.0 - Cross-Site Scripting
# Date: 2018-10-16
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: http://pokkho.com/lango/
# Software Link : http://pokkho.com/lango/auth/login
# Software : LANGO - Codeigniter Multilingual Script ...
```

Airties AIR5342 1.0.0.18 - Cross-Site Scripting
ismail Tasdelen
webapps 80

```
... # Exploit Title: Airties AIR5342 1.0.0.18 - Cross-Site Scripting
# Date: 25-09-2018
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: [https://www.airties.com/]
# Software [http://www.airties.com.tr/support/dcenter/]
# Version: [1.0.0.18]
# Affected products: AIR5342, AIR5343v2, AIR5443v2 ...
```

WordPress Plugin Support Board 1.2.3 - Cross-Site Scripting
ismail Tasdelen
webapps 80

```
... # Exploit Title: Wordpress Plugin Support Board 1.2.3 - Cross-Site Scripting
# Date: 2018-10-16
# Exploit Author: Ismail Tasdelen
```

You can see the exploits of İsmail Taşdelen with the author parameter.

platform:linux type:local

Shodan
Developer
Book
More...

SHODAN
Exploits
platform:linux type:local

Logout

TOTAL RESULTS
979

AUTHOR
Metasploit 31
anonymous 24
Juan Sacco 20
Google Security Research 15
Jon Oberheide 8

S.u.S.E Linux 4.x/5.x/6.x/7.0 / Slackware 3.x/4.0 / Turbolinux 6 / OpenLinux 7.0 - 'fdmount' Local Buffer Overflow (3)
War
local
... source: http://www.securityfocus.com/bid/1239/info
A buffer overflow exists in the 0.8 version of the fdmount program, distributed with a number of popular versions of Linux. By supplying a large, well crafted buffer containing machine execut

Rocks Clusters 4.1 - 'umount-loop' Local Privilege Escalation
Xavier de Leon
local
... #!/usr/bin/env python

rocksountdirty.py: Rocks release <=4.1 local root exploit
quick and nasty version of the exploit. make sure the . is writable and
you clean up afterwards. ;)

coded ...

ProFTPD 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (1)
Revenge
local
... #!/usr/bin/perl -w

\$Id: revenge_proftpd_ctrls_24.pl, v1.0 2007/02/18 19:24:22 revenge Exp \$

ProFTPD v1.3.0/1.3.0a Controls Buffer Overflow Exploit
[old style school sploit against gcc 3.x and linux kernel 2.4]

Original Advisory :
http://www.coresecurity.com/?action ...

PHP 5.2.1 - 'session_regenerate_id()' Double-Free
Stefan Esser
local
...
//
#####

With platform parameter you can see the exploits that work in the operating system, local or from afar.

You can also access webcams that have default passwords with Shodan.


Server:SQ-WEBCAM

SHODAN Server: SQ-WEBCAM

Exploits Maps Like 10,464 Download Results Create Report

TOTAL RESULTS: 98

TOP COUNTRIES



Country	Count
Germany	26
Netherlands	10
Italy	9
Poland	8
Hungary	8

TOP SERVICES

Service	Count
HTTP	49
HTTP (8080)	25
HTTP (83)	4
HTTP (81)	4
NAS Web Interfaces	2

TOP ORGANIZATIONS

Organization	Count
Deutsche Telekom AG	20
T-mobile Netherlands bv.	6
Wind Telecomunicazioni	4
Xs4all Internet BV	2
Telstra Internet	2

TOP PRODUCTS

Product	Count
dvr1614n web-cam httpd	91
Apache httpd	1

RELATED TAGS: webcam surveillance cams

62.93.33.23
PR2 Network
Address: 2018-12-02 11:26:51 GMT
Poland, Rzeszow
Details

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 434

79.60.165.245
Telecom Italia Business
Address: 2018-12-02 06:55:27 GMT
Italy, Naples
Details

HTTP/1.0 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 55

87.170.10.7
Deutsche Telekom AG
Address: 2018-12-02 03:34:16 GMT
Germany, Chemnitz
Details

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 518

Welcome to Network/IP Camera
121.211.179.68
ip: 121.211.179.68 ipui:
0-001-001-movetogood.net.au
Telstra Internet
Address: 2018-12-02 03:26:34 GMT
Australia, Dulwich Hill
Details

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 2747

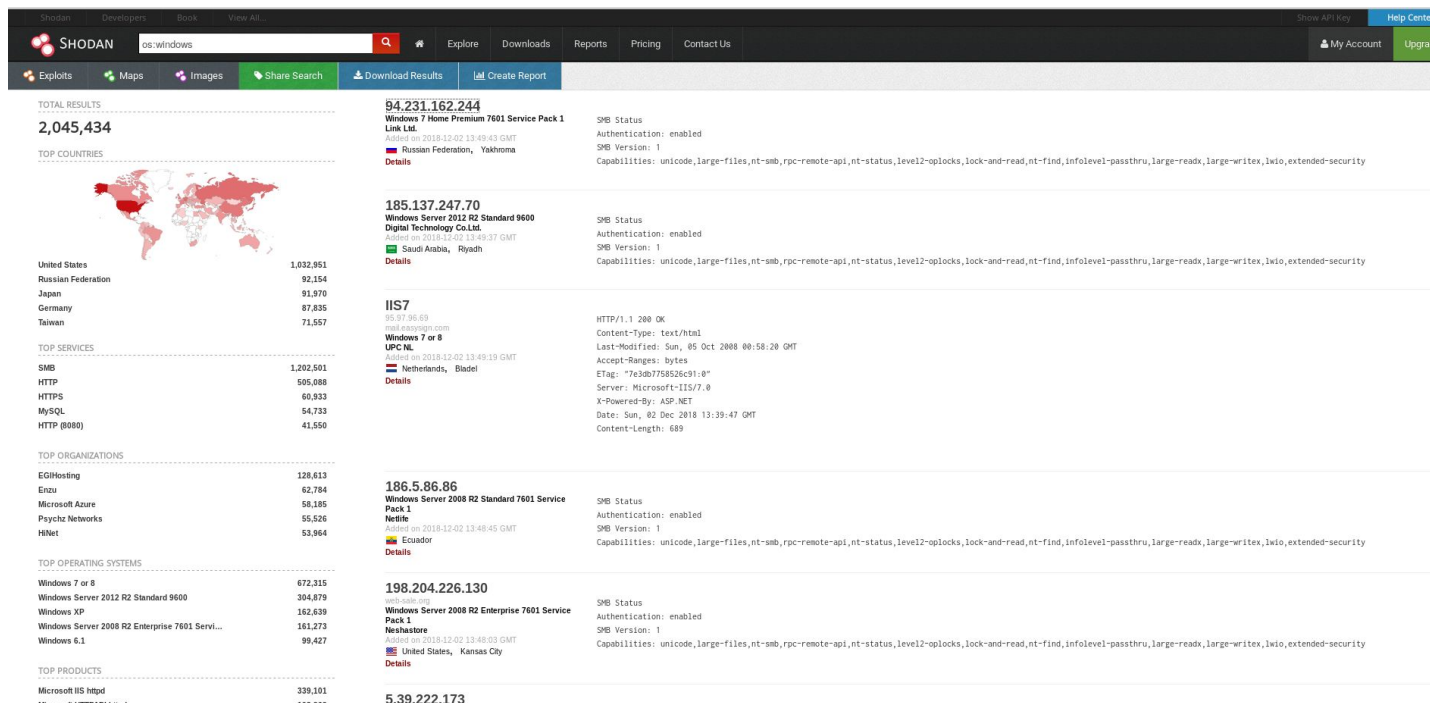
171.0.81.55
Starhub Mobile
Address: 2018-12-01 21:59:17 GMT
Singapore, Singapore
Details

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 344

You can see the top voted searches on the **explore** part in the Shodan menu.

OS Scanning

os:windows



Country

You can search in a specific country by typing their extensions in. As example: country:is (Iceland)

Shodan

Developers

Book

View All...

SHODAN

country.is

🔍

🏠

Explore

Downloads

Reports

Pricing

Contact Us

Show API Key

Help Center

🔗 Exploits

🗺 Maps

🖼 Images

👍 Like 2

📄 Download Results

📄 Create Report

My Account

Upgrade

TOTAL RESULTS

108,944

TOP COUNTRIES

Iceland	108,944
---------	---------

TOP CITIES

Reykjavik	60,822
Kópavogur	6,734
Ákureyri	5,736
Selfoss	2,354
Keflavík	1,321

TOP SERVICES

Modem Web Interface	26,247
HTTP	20,233
HTTPS	18,706
NTP	5,348
SSH	3,572

TOP ORGANIZATIONS

Siminn	20,227
Adventia Island ehf	15,746
Fjaraskipti ehf	12,472
EAMAN Customers	11,037
Vodafone Iceland	6,173

TOP OPERATING SYSTEMS

Linux 3.x	1,397
Linux 2.6.x	304
Windows 7 or 8	237
Windows Server 2012 R2 Standard 9600	84
FreeBSD 9.x	11

RELATED TAGS:

country.is

82.221.128.52

82.221.128.52

Adventia Island ehf

Added on 2018-12-02 13:51:36 GMT

🇮🇸 Iceland

Details

89.160.215.160

89.160.215.160

EAMAN Customers

Added on 2018-12-02 13:47:18 GMT

🇮🇸 Iceland, Kópavogur

Details

HTTP/1.1 401 Unauthorized

Connection: Keep-Alive

WWW-Authenticate: Digest realm="HuaweiHomeGateway", nonce="eb53cb2356833fcac4c297846f7b927d", qop="auth", algorithm="MD5"

Content-Length: 0

Velkomin í Saumakassann

212.30.204.43

212-30-204-43.static.simnet.is

Siminn

Added on 2018-12-02 13:44:30 GMT

🇮🇸 Iceland, Kópavogur

Technologies: jQuery Migrate animate.css PHP

Details

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 02 Dec 2018 13:44:30 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=20

Vary: Accept-Encoding

Link: <http://saumakassinn.is/wordpress/wp-json/>; rel="https://api.w.org/"

Link: <http://...

89.160.220.183

89.160.220.183

EAMAN Customers

Added on 2018-12-02 13:44:29 GMT

🇮🇸 Iceland, Reykjavik

Details

HTTP/1.1 401 Unauthorized

Connection: Keep-Alive

WWW-Authenticate: Digest realm="HuaweiHomeGateway", nonce="58d57e398545478e2b8f81a1a3c97b7", qop="auth", algorithm="MD5"

Content-Length: 0

89.160.145.173

89.160.145.173

Vodafone Iceland

Added on 2018-12-02 13:44:25 GMT

🇮🇸 Iceland, Reykjavik

Details

HTTP/1.1 401 Unauthorized

Connection: Keep-Alive

WWW-Authenticate: Digest realm="HuaweiHomeGateway", nonce="bad85d27e85548bc2bada8d8312f9e8", qop="auth", algorithm="MD5"

Content-Length: 0

City

Searching for systems in specific cities is possible as well.

The screenshot shows the Shodan search engine interface. The search query is 'city: washington'. The results are categorized into several sections:

- TOTAL RESULTS:** 571,782
- TOP COUNTRIES:** United States (561,051), United Kingdom (10,731)
- TOP SERVICES:** HTTPS (109,834), HTTP (109,442), SSH (47,760), 4587 (31,843), HTTPS (8443) (27,451)
- TOP ORGANIZATIONS:** Microsoft Azure (363,233), Reliabelhosting.com (30,598), Verizon Internet Services (28,049), Comcast Business (19,892), Comcast Cable (18,588)
- TOP OPERATING SYSTEMS:** Windows 7 or 8 (5,264), Linux 3.x (1,048), Windows Server 2012 R2 Datacenter 9600 (744), Linux 2.6.x (393), Windows Server 2016 Datacenter 14393 (109)
- TOP PRODUCTS:** Microsoft IIS httpd (63,716), OpenSSH (45,761), Microsoft HTTPAPI httpd (38,987), Apache httpd (24,935), ndmx (24,445)

The main content area displays three search results:

- Service Unavailable:** 23.96.23.61, Microsoft Azure, Issued on: 2018-12-02 13:52:00 GMT, Details: United States, Washington. SSL Certificate: Issued By: azuregateway, Issued To: azuregateway, Supported SSL Versions: TLSv1.2.
- 401 - Unauthorized: Access is denied due to invalid credentials.** 40.117.152.139, Microsoft Azure, Issued on: 2018-12-02 13:51:49 GMT, Details: United States, Washington. SSL Certificate: Issued By: Microsoft IT TLS CA 2, Issued To: Microsoft Corporation, Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2.
- Microsoft Azure Web App - Error 404:** 137.184.1.1, Microsoft Azure, Issued on: 2018-12-02 13:50:27 GMT, Details: United States, Washington. SSL Certificate: Issued By: Microsoft IT TLS CA 4, Issued To: Microsoft Corporation, Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2.

As you can see, Shodan gives us so many options. Let me give you an example along with the other parameters that I need to talk about:

country:is org:"EAMAN Customers" product:MySQL


Shodan Developers Book View All...

SHODAN country:is org:"EAMAN Customers" product:mysql

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
1

TOP COUNTRIES



Iceland 1

TOP CITIES

Kópavogur 1

TOP ORGANIZATIONS

EAMAN Customers 1

TOP VERSIONS

5.1.73-Ubuntu0.10.04.1 1

89.160.162.171
89.160.162.171:8080
EAMAN Customers
Running on 2018-11-30 02:31:28 GMT
Iceland, Kópavogur
Details

database

5.1.73-Ubuntu0.10.04.1

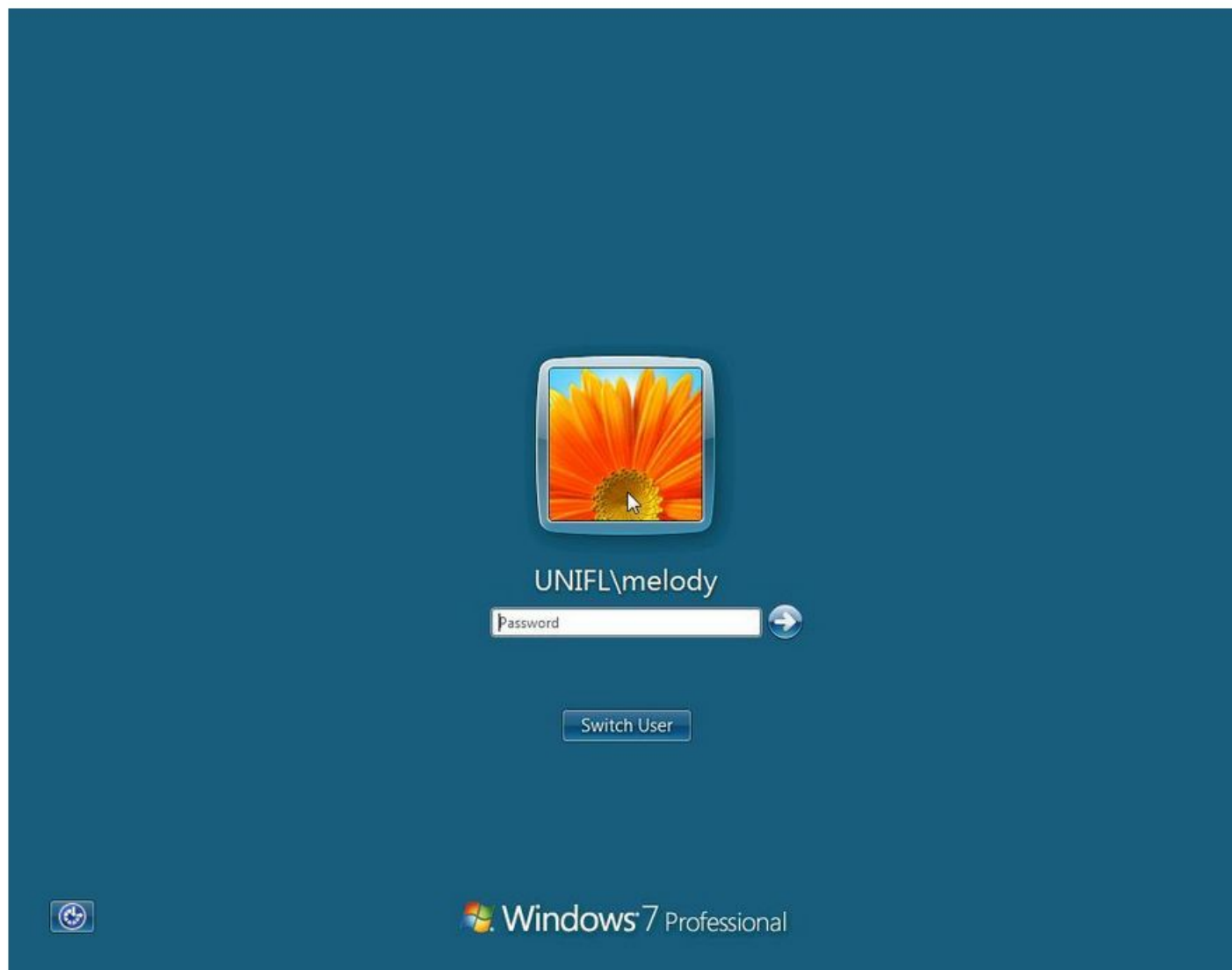
© 2013-2018, All Rights Reserved - Shodan®

With this, I searched for EAMAN Customers in Iceland's devices using MySQL but I wish I didn't find this device. I have never seen this many vulnerabilities together in a device before. 😊 And if the 3389th (Remote Desktop Protocol) port is open on it, don't be surprised if you're faced with the login screen right away. 😊

3389
tcp
rdp

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00



Hope you liked it!

Tags: [cyber security](#) [shodan](#)

Previous Post

 **Developing Apps Without Coding Knowledge**

Next Post

 **Penetration Test Steps**

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

POST COMMENT

Search...



Archives

August 2019

July 2019

June 2019

May 2019

April 2019

March 2019

February 2019

January 2019

December 2018

November 2018

October 2018

September 2018

August 2018



KernelBlog

© 2019 KERNELBLOG - En.KernelBlog.org & KernelBlog.org KernelBlog.

Navigate Site

Home / **Turkish** / **Cyber Security** / **Linux** / **Windows** /
Mobile / **Science** / **Tool Introduction** / **Other** / **About Us** /
Contact

Follow Us

