

CYBR 352 Week 9 Lab

- Access <https://www.shodan.io> and Login or Register a Shodan Academic Plus account with your canton.edu email address.

The screenshot shows the Shodan Account Overview page. The top navigation bar includes links for Shodan, Maps, Images, Monitor, Developer, and More. The account menu is open, showing options like Account, Overview, Billing, Take a Tour, and Log out. The left sidebar contains links for Overview, Settings, Change Password, and Redeem Gift Code. The main content area displays the Account Overview with the following details:

Account Level	Academic membership
Display Name	MarcoCanton
Email	gonza313@canton.edu
Member	Yes
API Key	Show

- Try two simple searches and show some device details.
Windows Server 2022

The screenshot shows the Shodan search results for the query "Windows Server 2022". The top navigation bar includes links for Shodan, Explore, Downloads, Pricing, and a search icon. The account menu is open, showing options like Account. The left sidebar displays the total results (911,807) and a world map showing the top countries. The main content area shows the search results for the IP address 217.160.48.149, which is located in Germany, Stuttgart. The results include a list of top countries and a detailed view of the device details.

TOTAL RESULTS
911,807

TOP COUNTRIES

Country	Count
China	226,867
United States	211,389
Germany	79,351
Japan	45,442
Singapore	36,415

[More...](#)

TOP PORTS

217.160.48.149

1&1 IONOS SE
Germany, Stuttgart

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

HTTP/1.1 401 Unauthorized
Server: Microsoft-IIS/10.0
WWW-Authenticate: Digest qop="auth",algorithm=MD5-sess,nonce="+Upgraded+v1114cb33aafe304136b9eb3dc33fb9bb2aafd8f6bad84",
WWW-Authenticate: Negoti...

1.14.250.114

Tencent cloud computing (Beijing) Co., Ltd.
China, Shenzhen

self-signed

SSL Certificate

Issued By:
J-Common Name:

Issued To:
J-Common Name:

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

Remote Desktop Protocol
\\x03\\x00\\x00\\x13\\x0e\\x00\\x00\\x124\\x00\\x02\\x1f\\x00\\x02\\x00\\x00\\x00

Remote Desktop Protocol NTLM Info:
OS: **Windows Server 2022**
OS Build: 10.0.20348
Target Name: 10_0_20_14
NetBIOS Domain Name: 10_0_20_14
NetBIOS Computer Name: 10_0_20_14
DNS Domain Name: ...

Marco Gonzalez

[illegible]

Raspberry Pi

SHODAN

Explore

Downloads

Pricing


Raspberry Pi

Account

TOTAL RESULTS

382

TOP COUNTRIES



China102

United States44

Germany32

France31

United Kingdom22

More...

8.137.121.14

Aliyun Computing Co.LTD

China, Chengdu

cloud

217.129.88.68

se-217-129-88-68.netvli.sao.pt

NOWO COMMUNICATIONS, S.A.

Portugal, Oliveira do Hospital

HTTP/1.1 200 OK

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

Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647

Set-Cookie: i_like_gogs=13b0ffa8a3df8af; Path=/; HttpOnly

Set-Cookie: _csrf=Gty_1Iabtggv0-0K6SU0mfmfxQw6RTcxHjAytzHwNTczRTUxhY0MQ; Path=/; Domain=192.168.50.127; Expires=Wed, 1

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

View Report

Download Results

Historical Trend

Browse Images

View on Map

8.137.121.14

Regular View

Raw Data

Tags: cloud, eat-product

General Information

Cloud Provider

Alibaba Cloud

Country

China

City

Chengdu

Organization

Aliyun Computing Co.LTD

ISP

Hangzhou Alibaba Advertising Co.,Ltd.

ASN

AS537963

Vulnerabilities

CVE-2023-51767

OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: This is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

Open Ports

22, 80, 2222, 8889, 9090, 9999, 50000

22 / TCP

46825813 | 2024-03-28T09:55:13, 766853

OpenSSH / 4

SSH-2.0-OpenSSH_7.4

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQCAwEAAQFmhuYUhpPQWc3p4dUlhWdA12dPQdJ09

extGd1T23S8m0w0dA0770WvY2Kw0w06W070dA04r0FFv4d0St0/Scy3JAC0M01C07

qk0d0Rn0d0vY8j7Bv8tPj0P20vY7d0d0M0v0k0Fv5G0I7Z/rp0M0/jg0d0k0u0w0e12u

TPv7u0v0v/Cwb1j9u0A7A0v52u0y1800w0y0JfQj8J0d0w0Pj0q0Z0vJ0d0I0d0u0k000m1

64fUj37g0d0Q1wCP0E90M0y0816f1A0Z0u0A50v0cYn3PFR0R11c0M0k0tk0vVLC2T

FingerPrint: Fe14a0e1301921291801401ad1791e3191e190137

Key Algorithms:

curve25519-sha256

curve25519-sha256@libssh.org

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256

diffie-hellman-group16-sha512

diffie-hellman-group18-sha512

diffie-hellman-group-exchange-sha1

diffie-hellman-group14-sha256

diffie-hellman-group14-sha1

diffie-hellman-group1-sha1

Server Host Key Algorithms:

217.129.88.68 Regular View Raw Data

// TAGS: not-product // LAST SEEN: 2024-04-02

General Information

Hostnames: se-217-129-88-68.netvisao.pt, photuseretratus.pt, daemon.photuseretratus.pt

Domains: NETVISAQ.PT, PHOTUSERETRATUS.PT

Country: Portugal

City: Oliveira do Hospital

Organization: NOWO COMMUNICATIONS, S.A.

ISP: NOWO COMMUNICATIONS, S.A.

ASN: AS13156

Open Ports

80, 443, 445, 8989

// 80 / TCP

1964976744 | 2024-03-31T08:57:45.186869

nginx 1.22.1

HTTP/1.1 404 Not Found
Server: nginx/1.22.1
Date: Sun, 31 Mar 2024 08:57:44 GMT
Content-Type: text/html
Content-Length: 555
Connection: keep-alive

// 443 / TCP

1326887972 | 2024-03-27T00:45:43.808532

nginx 1.22.1

HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Wed, 27 Mar 2024 00:45:43 GMT
Content-Type: text/html
Content-Length: 34300
Last-Modified: Wed, 13 Dec 2023 23:04:25 GMT
Connection: keep-alive
ETag: "d2fa3879-8bfc"
Accept-Ranges: bytes

Web Technologies

CDN: Unpkg

JavaScript Libraries: jQuery 3.6.0

- Try two advanced searches with search filters
ssh port:22, 3333

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing ssh port:22,3333 Account

TOTAL RESULTS: 21,322,798

TOP COUNTRIES

United States	5,899,741
China	2,280,958
Germany	1,930,049
Brazil	1,870,579
Singapore	750,883

More...

101.43.10.131

Tencent Cloud Computing (Beijing) Co., Ltd

China, Shanghai

cloud

SSH-2,0-OpenSSH_7.4

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQDQevhvkTu0PcDgyzptqCyKJh/qGZR/jGiuFkdWzZTHPdu51FyOxUyJlhYKtbKpPhLMQIIELE-NiikZbdPIFaeIp8aE38R1vS-zlojs/1qvWj0nbR6Sgi/1fE8RahyXtdD25RH0vCyE0M4poPzzID78V61pq1I1Vek1aGskxRE0M100D4agCJLR+/AN7G7CH+A0NSAOp0whkSxb3RR2pWVfhsJ1xbF/j...

2024-04-02T05:13:33.525788

8,222,134,160

Alibaba Cloud (Singapore) Private Limited

Singapore, Singapore

cloud

SSH-2,0-OpenSSH_7.4

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQCT0GdW4yBfhW/do2pTzK2j5c2F119zr7Q6e0AgcZ2peVMPubZEEZTXF5pXfWqk0T10rwcG8FaQhKX/ttq/58Mc9nq/GzqPMK3nmP1YxJBh859ApFzGA7szgUQuDWhzCBYDBARYLz31pZUK5Tdruv/rngzGEaFAfMfOYJQ5upvYthG+D+zgEkowzskFm5u9DgZV5L9AebXbag2zrz33e7dq...

2024-04-02T05:10:20.465646

https://www.shodan.io/search/report?query=ssh+port%3A22%2C3333

Marco Gonzalez

101.43.10.131

Regular View

> Raw Data

Tags: cloud

General Information

Hostnames

ipinxuanyi.com

Domains

PINXUANYI.COM

Cloud Provider

Tencent Cloud

Country

China

City

Shanghai

Organization

Tencent Cloud Computing (Beijing) Co., Ltd

ISP

Shenzhen Tencent Computer Systems Company Limited

ASN

AS45090

Vulnerabilities

CVE-2023-51767

OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: This is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

Open Ports

22

80

443

8888

22 / TCP

OpenSSH 7.4

SSH-2.0-OpenSSH_7.4

Key: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQ=

Fingerprint: e1af2d27c576bd8b7a37f2ba8a18148a5

Server Host Key Algorithms

Tags: cloud self-signed

General Information

Cloud Provider

Alibaba Cloud

Country

Singapore

City

Singapore

Organization

Alibaba Cloud (Singapore) Private Limited

ISP

Alibaba (US) Technology Co., Ltd.

ASN

AS45102

Vulnerabilities

CVE-2023-51767

OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: This is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

Open Ports

22

443

22 / TCP

OpenSSH 7.4

SSH-2.0-OpenSSH_7.4

Key: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQ=

Fingerprint: 7313d691b4da25b4b5a1a58791cc07781c

Server Host Key Algorithms

hostname:canton.edu

[illegible]

Marco Gonzalez

[illegible]

- Try two searches with Shodan Explore
product:Minecraft

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Downloads

Pricing

product.minecraft

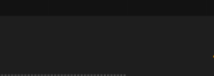
Q

Account

TOTAL RESULTS

202,095

TOP COUNTRIES



United States	72,252
Germany	34,543
Japan	14,979
Canada	10,410
China	8,935
More...	

View Report

Download Results

Historical Trend

View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

188.212.103.148

s3-148.gazdarejocan.ro

o

TELESYSTEM SRL

Romania, Bacău

videogame

Minecraft Server:

Version: 1.20.1 (Protocol 763)

Description: A Minecraft Server

Online Players: 0

Maximum Players: 20

2024-04-02T05:16:38.245422

116.82.80.252

fp745250fc.knqe108.a.p.nuro.jp

So-net Service

Japan, Kawasaki

videogame

\xbc\x01\x1a\xb9\x01["translate":"disconnect.genericReason", "with":["Internal Exception: io.netty.handler.codec.Decode

2024-04-02T05:15:18.794216

64.225.245.194

Server Pro Sweden AB

Minecraft Server:

2024-04-02T05:13:48.515075

188.212.103.148

ArdeonaniStrugeniLutzuCalugaraAjacuCiuheneCoteniUnqueni

OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors

Regular ViewRaw Data

// TAGS: databaseeol-productvideogame

General Information

Hostnames	s3-148.gazduirejocuri.ro
Domains	GAZDUIREJOCURI.RO
Country	Romania
City	Bacău
Organization	TELESYSTEM SRL
ISP	Annnary SRL
ASN	AS39383

Vulnerabilities

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

CVE-2023-44487

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Open Ports

2280330625565

// 22 / TCP

OpenSSH 8.9p1 Ubuntu-3ubuntu0.6

```

SSH-2.0-OpenSSH_8.9p1_Ubuntu-3ubuntu0.6
Key Type: ecdsa-sha2-nistp256
Key: AAAAE2VjZDBhLnRoY1ltbmIzOHAyMTYAAABlcmIzOHAyMTYAAABBCNjBj7n36iockrr3Tomu
Fcyj8MaJysHkPjRA6tlygh4tgL2Lf2HERey8fapNFYVffqzv0996lakTK4Q+
FingerPrint: c916154:f51d6e07:c14b:e6168:48:e1:831d:2b

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
untrap701z25519-sha512@openssh.com
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256
hex:strict-s-van@openssh.com

Server Host Key Algorithms:
rsa-sha2-512
rsa-sha2-256
ecdsa-sha2-nistp256
ssh-ed25519

```

116.82.80.252

ArdeonaniStrugeniLutzuCalugaraAjacuCiuheneCoteniUnqueni

OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors

Regular ViewRaw Data

// TAGS: videogame

General Information

Hostnames	poeponemdns.bzwww.poeponemdns.bzf745250fc.kngel08.ap.nuro.jp
Domains	MYDNS.BZNURO.JP
Country	Japan
City	Kawasaki
Organization	So-net Service
ISP	Sony Network Communications Inc.
ASN	AS2527

Web Technologies

JavaScript Frameworks	Static Site Generator
Nuxt.js	Nuxt.js

Open Ports

53	80	81	82	83	84	88	102	104	111	135	175
179	389	427	443	548	631	789	1024	1311	1400	1433	1471
1723	1741	1800	1801	1911	1925	1935	1962	2082	2086	2222	2346
2375	2404	2480	2761	2762	3000	3050	3128	3260	3268	3388	3389
3541	3542	3689	3749	4040	4157	4242	4369	4500	4567	4664	4782
4786	4848	5000	5005	5009	5222	5269	5357	5555	5560	5601	5800
5801	5900	5901	5985	6080	6664	6668	7171	7474	7547	7657	7777
7779	7989	8000	8001	8008	8010	8060	8069	8080	8086	8087	8090
8098	8112	8123	8206	8291	8334	8554	8728	8800	8888	9000	9009
9080	9090	9191	9206	9295	9418	9595	9800	9860	9876	9944	9981
9999	10001	10134	10243	10554	11112	11371	13579	14285	16892	19000	19071

Server: boa WWW-Authenticate: Camera (a list of cameras with default credentials)

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Downloads

Pricing

server: boa WWW-Authenticate: Camera

Account

TOTAL RESULTS

3,231

TOP COUNTRIES

Spain536

Germany273

Russian Federation264

Argentina193

Netherlands146

More...

View Report

Download Results

Historical Trend

View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

118.193.31.179

UCUL-JP

Japan, Tokyo

honeypot

HTTP/1.1 200 OK

Server: MiniUPnPd/1.4

Pragma: no-cache

Cache-Control: no-cache

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

Content-Length: 55860

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/tr/xhtml1/DTD/xhtml1-Transitional.dtd">

<html xmlns="http://www.w3.org/199...

2024-04-02T05:08:01.645359

109.104.153.125

oneprovider.com - Amsterdam Infrastructure

Netherlands, Amsterdam

HTTP/1.1 200 OK

Server: MiniUPnPd/1.4

Pragma: no-cache

Cache-Control: no-cache

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

2024-04-02T05:07:28.190462

118.193.31.179

Regular View

Raw Data

Images

Video

Setagaya

Minato

Koto

// TAGS: database eol-product honeypot bot self-signed vpn

// LAST SEEN: 2024-04-02

General Information

CountryJapan

CityTokyo

OrganizationUCUL-JP

ISPCDS Global Cloud Co., Ltd

ASNAS63199

Web Technologies

JavaScript Frameworks

JavaScript Libraries

AngularJS

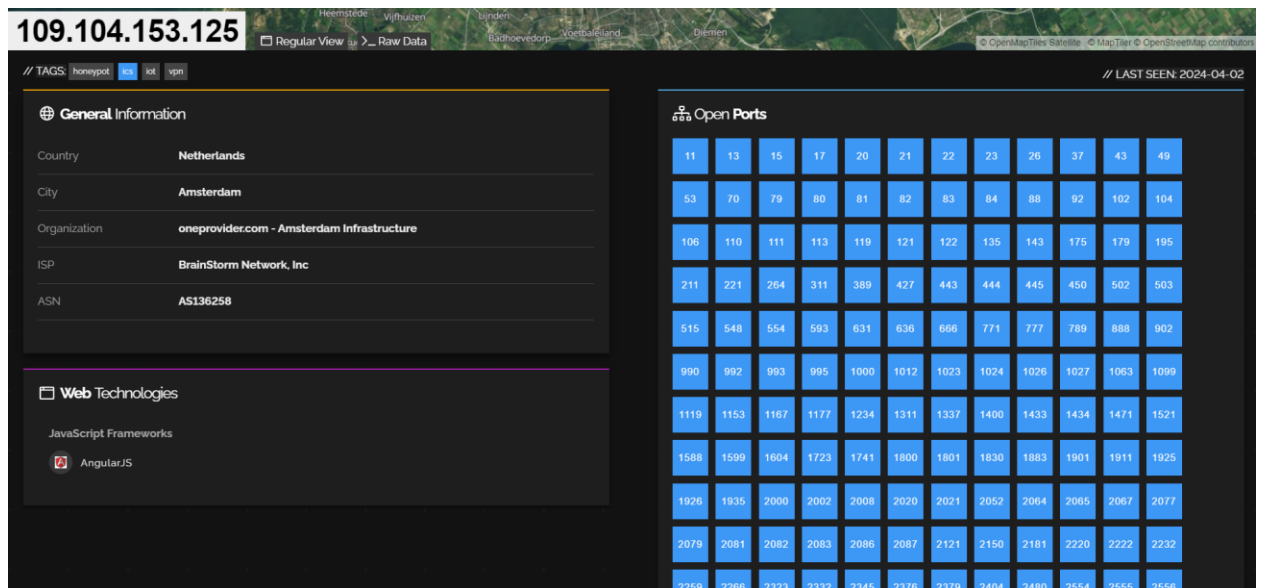
Prototype

jQuery

Vulnerabilities

Open Ports

11	13	15	17	19	21	22	23	26	37	43	49
53	70	79	80	81	82	83	84	88	90	96	104
110	111	113	119	122	131	135	139	143	175	179	195
211	221	283	284	311	389	427	443	444	445	449	465
503	515	548	554	587	593	631	636	646	666	675	771
789	873	902	943	992	993	994	995	1012	1023	1024	1026
1027	1099	1111	1119	1153	1167	1177	1234	1290	1311	1337	1400
1433	1471	1500	1521	1599	1604	1660	1723	1741	1800	1801	1820
1883	1901	1911	1925	1926	1935	1950	1951	1962	2000	2002	2008
2012	2020	2022	2050	2051	2054	2055	2061	2063	2067	2068	2080
2081	2082	2083	2086	2087	2121	2154	2181	2222	2323	2332	2345



What I learned from exploring Shodan search results is that many critical devices connected to the internet are available to be viewed by just anyone. Many of the results I found had configurations or versions containing vulnerabilities that hackers can abuse. One idea against Shodan hacking is to use fire to fight fire. Check your networks and devices through Shodan to see if any results pop up. We can find vulnerabilities in our networks and quickly patch them up from the results. One other idea against Shodan hacking is to use VPN to access any part of the network so that Shodan can't find any of the devices.