Lab Report No.2

Shodan.io

Ethical Hacking

Submitted By: Raghad Alharthi 2210003220

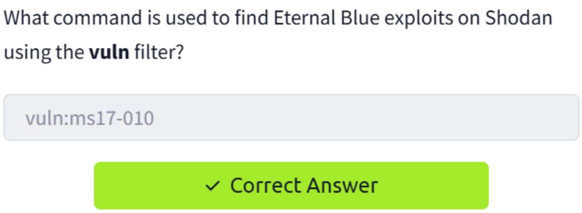
Section: CS Group no. 2

Contents

Room: Shodan.io

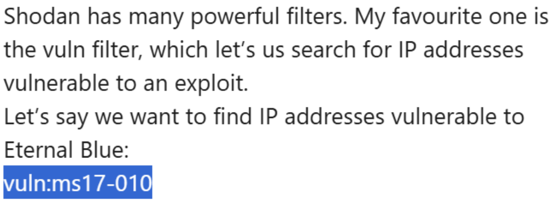
Task 2

Q1



What command is used to find Eternal Blue exploits on Shodan using the **vuln** filter?

vuln:ms17-010

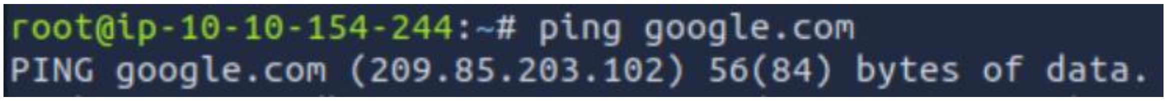


Shodan has many powerful filters. My favourite one is the vuln filter, which let's us search for IP addresses vulnerable to an exploit.
Let's say we want to find IP addresses vulnerable to Eternal Blue:
vuln:ms17-010

Task 3

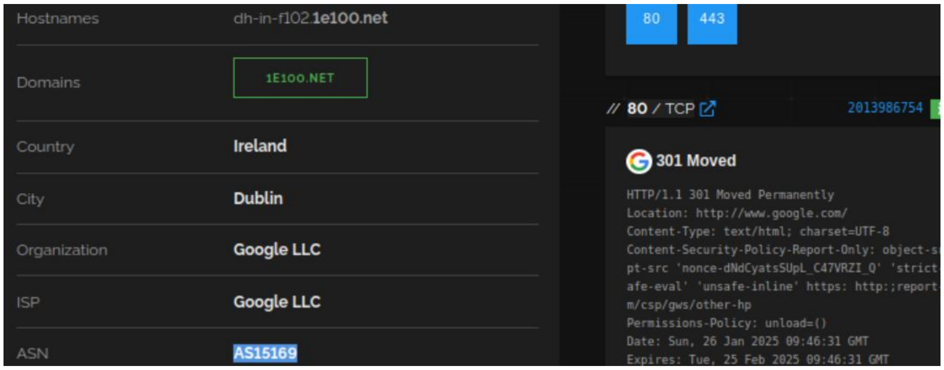
Q1

1- Get IP for Google from terminal



```
root@ip-10-10-154-244:~# ping google.com
PING google.com (209.85.203.102) 56(84) bytes of data.
```

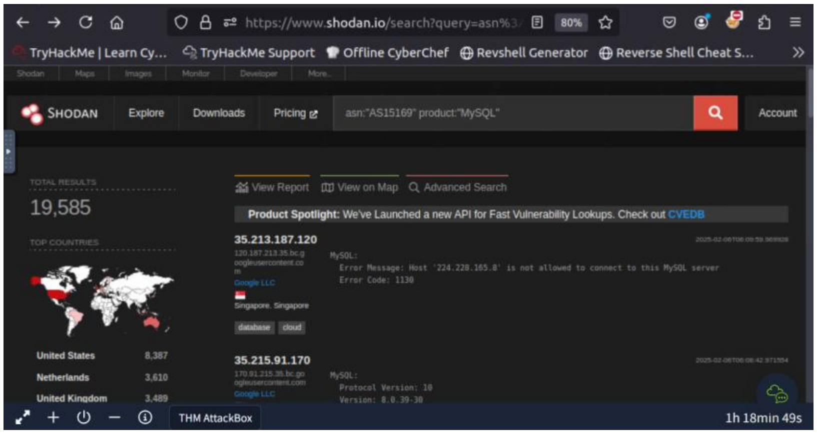
2- Search IP and get Google's ASN



Hostnames	dh-in-f102.1e100.net
Domains	1E100.NET
Country	Ireland
City	Dublin
Organization	Google LLC
ISP	Google LLC
ASN	AS15169

```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-s
pt-src 'nonce-dNdCyatsSUpL_C47VRZI_Q' 'strict
afe-eval' 'unsafe-inline' https: http:;report
m/csp/gws/other-hp
Permissions-Policy: unload=()
Date: Sun, 26 Jan 2025 09:46:31 GMT
Expires: Tue, 25 Feb 2025 09:46:31 GMT
```

3- No proper output is showing.



asn:"AS15169" product:"MySQL"

TOTAL RESULTS
19,585

TOP COUNTRIES

United States	8,387
Netherlands	3,610
United Kingdom	3,489

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

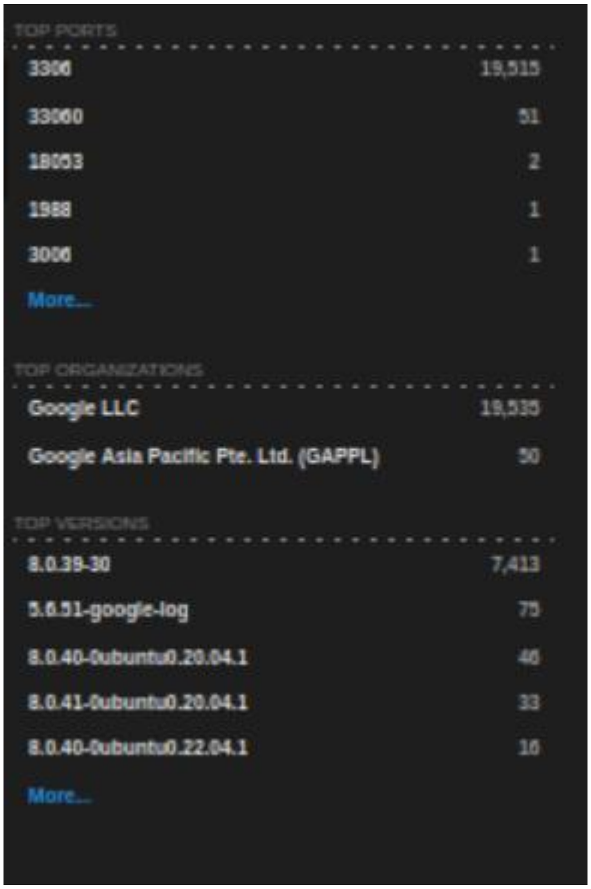
35.213.187.120
120.187.213.35.bc.googleusercontent.com
Google LLC
Singapore, Singapore
database cloud

```
MySQL:
  Error Message: Host '224.228.165.8' is not allowed to connect to this MySQL server
  Error Code: 1130
```

35.215.91.170
170.91.215.35.bc.googleusercontent.com
Google LLC

```
MySQL:
  Protocol Version: 10
  Version: 8.0.39-30
```

4- Filters showing:

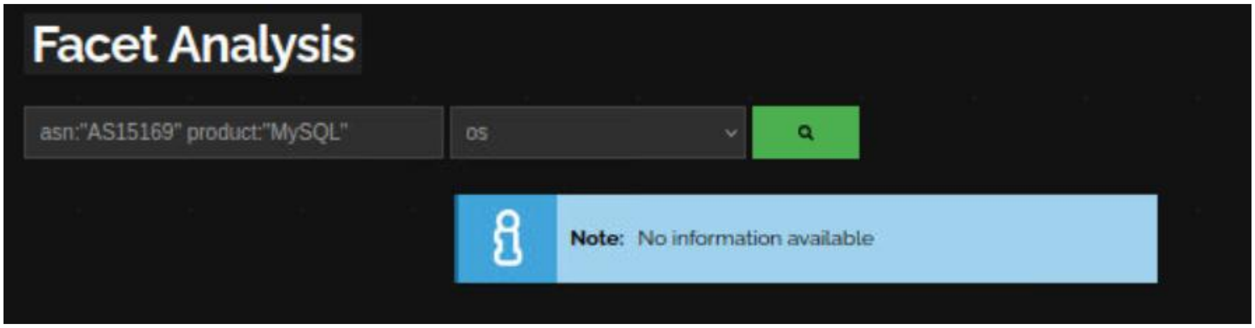


TOP PORTS	
3306	19,515
33060	51
18053	2
1988	1
3006	1
More...	

TOP ORGANIZATIONS	
Google LLC	19,535
Google Asia Pacific Pte. Ltd. (GAPPL)	50

TOP VERSIONS	
8.0.39-30	7,413
5.6.51-google-log	75
8.0.40-0ubuntu0.20.04.1	46
8.0.41-0ubuntu0.20.04.1	33
8.0.40-0ubuntu0.22.04.1	16
More...	

5- Even when filtering for OS show no result



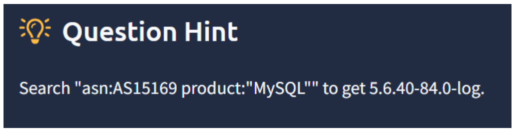
Facet Analysis

asn:"AS15169" product:"MySQL"

os

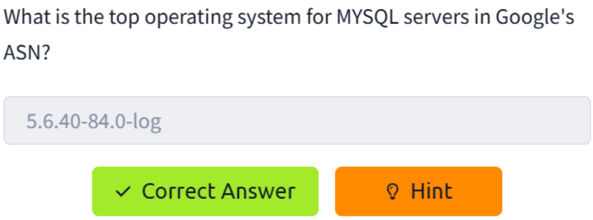
Note: No information available

6- Got answer from hint and found no proper answer.



Question Hint

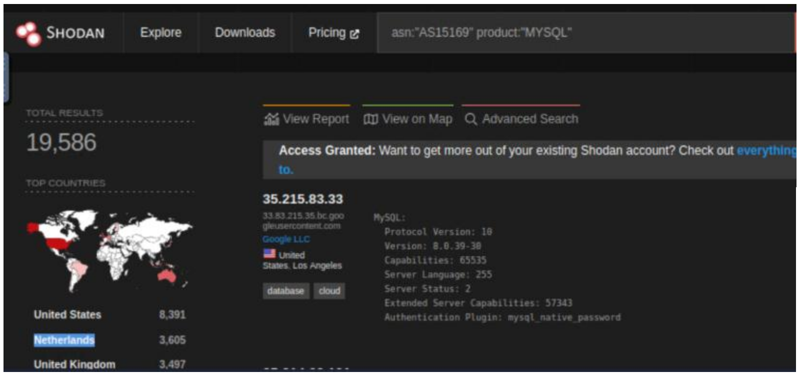
Search "asn:AS15169 product:"MySQL"" to get 5.6.40-84.0-log.



What is the top operating system for MYSQL servers in Google's ASN?

5.6.40-84.0-log

Q2



asn:"AS15169" product:"MYSQL"

TOTAL RESULTS

19,586

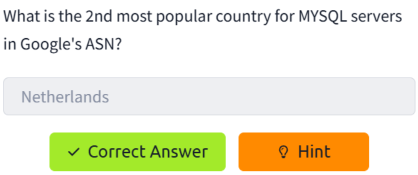
Access Granted: Want to get more out of your existing Shodan account? Check out everything to.

TOP COUNTRIES

United States	8,391
Netherlands	3,605
United Kingdom	3,497

35.215.83.33
33.83.215.35.bc.googleusercontent.com
Google LLC
United States, Los Angeles

```
MySQL:
  Protocol Version: 10
  Version: 8.0.39-30
  Capabilities: 65535
  Server Language: 255
  Server Status: 2
  Extended Server Capabilities: 57343
  Authentication Plugin: mysql_native_password
```

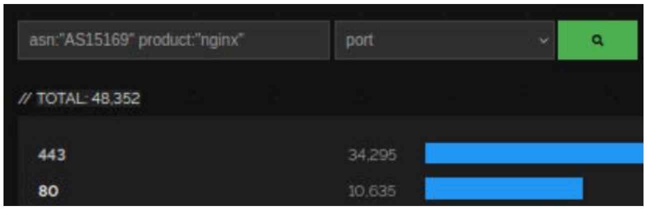


What is the 2nd most popular country for MYSQL servers in Google's ASN?

Netherlands

Q3

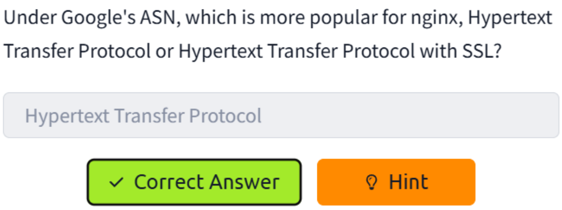
443 == HTTPs



asn:"AS15169" product:"nginx" | port

// TOTAL: 48,352

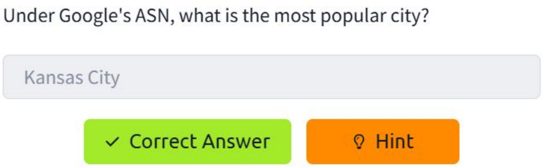
443	34,295
80	10,635



Under Google's ASN, which is more popular for nginx, Hypertext Transfer Protocol or Hypertext Transfer Protocol with SSL?

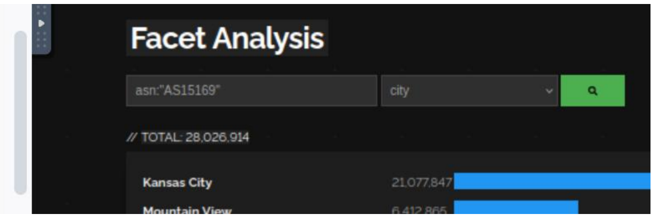
Hypertext Transfer Protocol

Q4



Under Google's ASN, what is the most popular city?

Kansas City



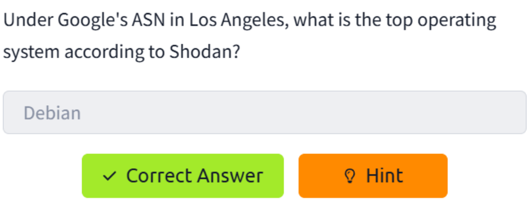
Facet Analysis

asn:"AS15169" | city

// TOTAL: 28,026,914

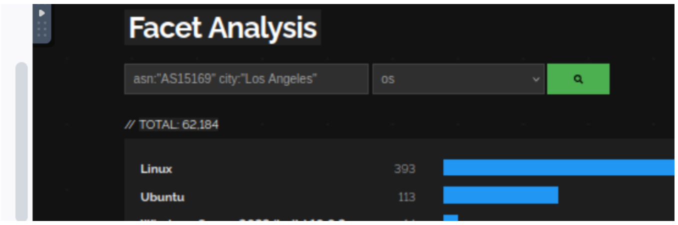
Kansas City	21,077,847
Mountain View	6,412,865

Q5



Under Google's ASN in Los Angeles, what is the top operating system according to Shodan?

Debian



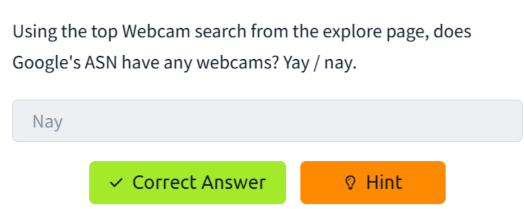
Facet Analysis

asn:"AS15169" city:"Los Angeles" | os

// TOTAL: 62,184

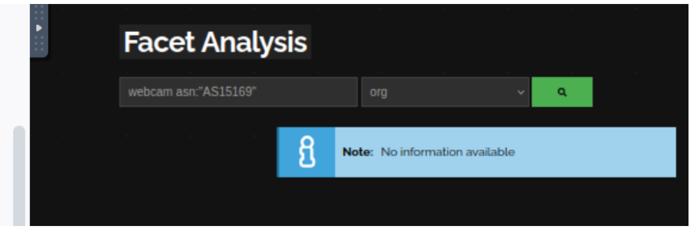
Linux	393
Ubuntu	113

Q6



Using the top Webcam search from the explore page, does Google's ASN have any webcams? Yay / nay.

Nay

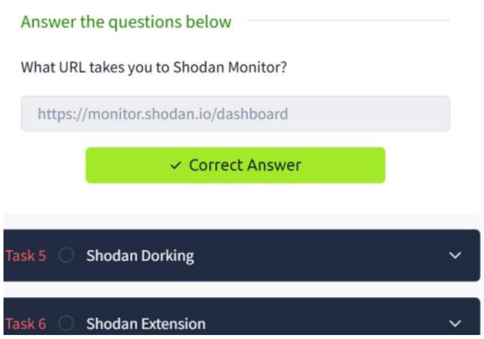


Facet Analysis

webcam asn:"AS15169" | org

Note: No information available

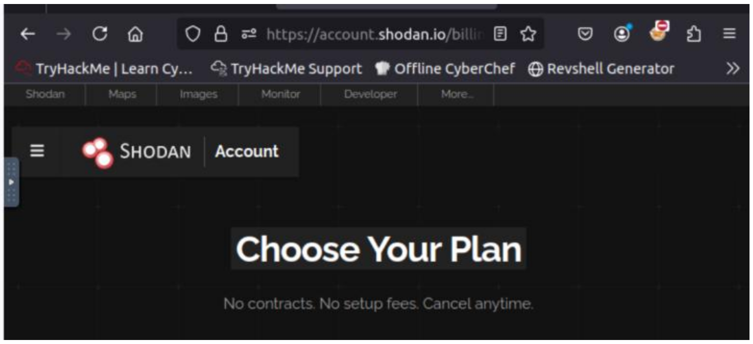
Task 4



Answer the questions below

What URL takes you to Shodan Monitor?

https://monitor.shodan.io/dashboard



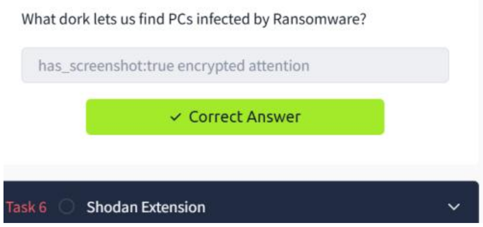
https://account.shodan.io/billin

Choose Your Plan

No contracts. No setup fees. Cancel anytime.

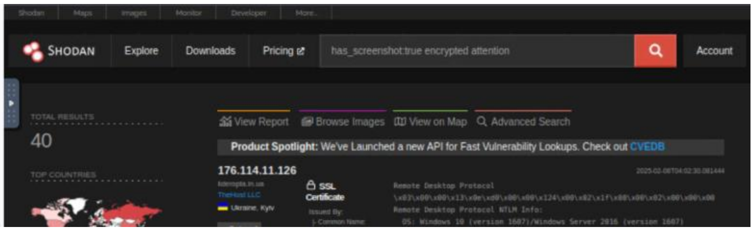
wouldn’t let me visit the url as I have to be subscribed to one of their plans.

Task 5



What dork lets us find PCs infected by Ransomware?

has_screenshot:true encrypted attention



has_screenshot:true encrypted attention

TOTAL RESULTS

40

TOP COUNTRIES

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

176.114.11.126

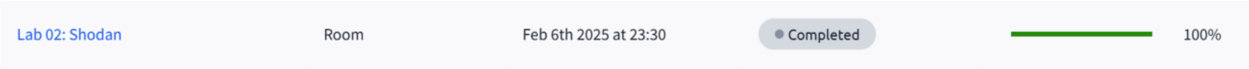
TheHost LLC

Ukraine, Kyiv

SSL Certificate

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)
```

Room Completed!



Lab 02: Shodan	Room	Feb 6th 2025 at 23:30	● Completed		100%