DEF CON

DC 0471 TRIVANDRUM

How I pwned Google´s Network Devices!

29th September, 2018

$whoami

- Sreeram KL - @KL_Sree
- High School Student,Web Security enthusiast and Bug bounty hunter.
- Currently Ranked 39th position in the world and 2nd in India on Google Hall of Fame.

What this talk is about?

IT'S A COMPLETE WASTE OF MY TIME
i-want-to-be-loved-by-you-alone.tumblr.com

The recon, methods,tools and stuffs used while hacking into Google's Network System for the 2nd time.

Yes I did it before. You can read it here: https://bit.ly/2xwPRm8

How it all started

By an accident!

THE RECON

How do I find another device’s IP?

After hours of Googling how to stuffs, the journey ended in ASN.

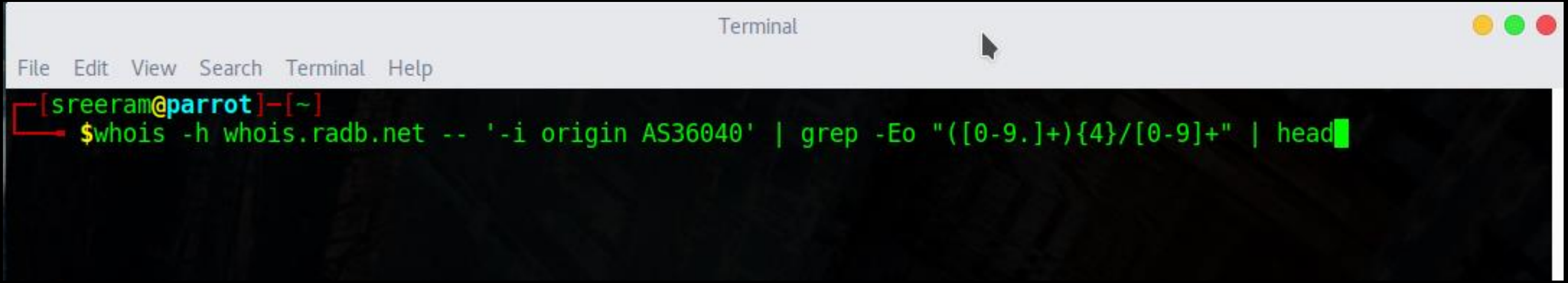
What is ‘ASN’?

ASN (Autonomous System Number) is a collection of IP routing prefixes under the control of one network or a company.(To get more confused refer the wikipedia definition of ASN)

It looks like (AS15169)

How to find IP from ASN?

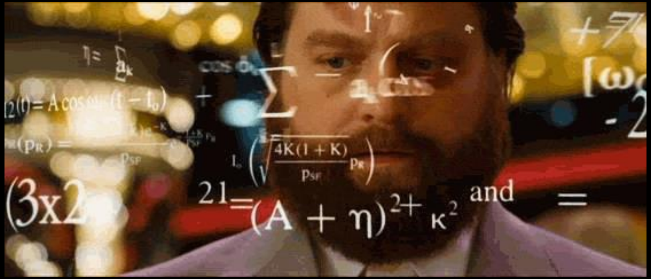
The IP ranges/ subnet can be extracted from ASN through "**whois**" tool as follows.



```
┌─[sreeram@parrot]─[~]
└──╼ $whois -h whois.radb.net -- '-i origin AS36040' | grep -Eo "([0-9.]+){4}/[0-9]+" | head
```

Finally We got the IP ranges

It's just the beginning:

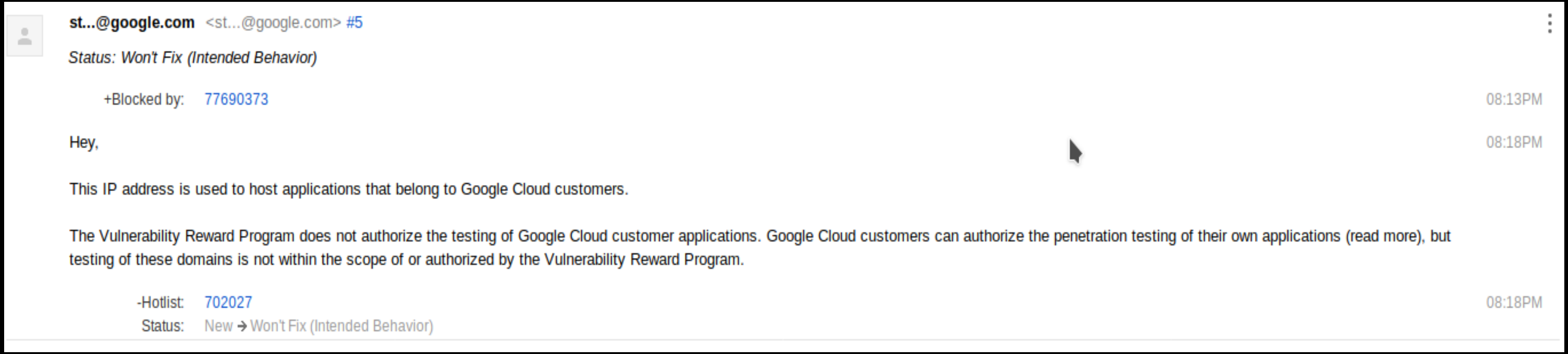


- Google have more than 100 different ASN.
- Most ASN have more than 50 ranges.
- Many IP ranges have more than 800 unique IP (some was even 7k)
- So we have about 100*50*800= 4000000, We have approximately 4000000 IP's to lookup....

I WAS LIKE! :|

Days passed on…….

One day, I found this screenshot on Facebook.



st...@google.com <st...@google.com> #5

Status: Won't Fix (Intended Behavior)

+Blocked by: 77690373 08:13PM

Hey, 08:18PM

This IP address is used to host applications that belong to Google Cloud customers.

The Vulnerability Reward Program does not authorize the testing of Google Cloud customer applications. Google Cloud customers can authorize the penetration testing of their own applications (read more), but testing of these domains is not within the scope of or authorized by the Vulnerability Reward Program.

-Hotlist: 702027 08:18PM
Status: New → Won't Fix (Intended Behavior)

Maybe Thanos Was Right

Now we have a lead!

Now we can eliminate the IP's that belongs Google Cloud and Google Fibre (Google's internet providing service) from our list.

How to sort out such a big list:

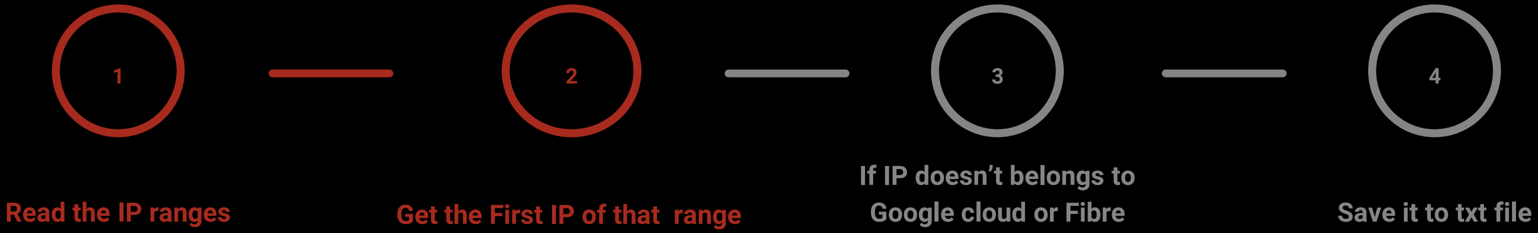
Bash to the rescue! I made a simple bash code that sort the IP that doesn't belong to Google Cloud and Google Fiber. But still we have 40 lac IP to sort out.

Again I was lucky!

Google have similar kind of IP in one subnet. So I didn't want to extract all IP and check if each one belongs to Google cloud or not. For this I just need to check the first Ip of each range. For this part my target shrinked

100*50=5000

IP segregation



1

Read the IP ranges

2

Get the First IP of that range

3

If IP doesn’t belongs to Google cloud or Fibre

4

Save it to txt file

Lucky again!

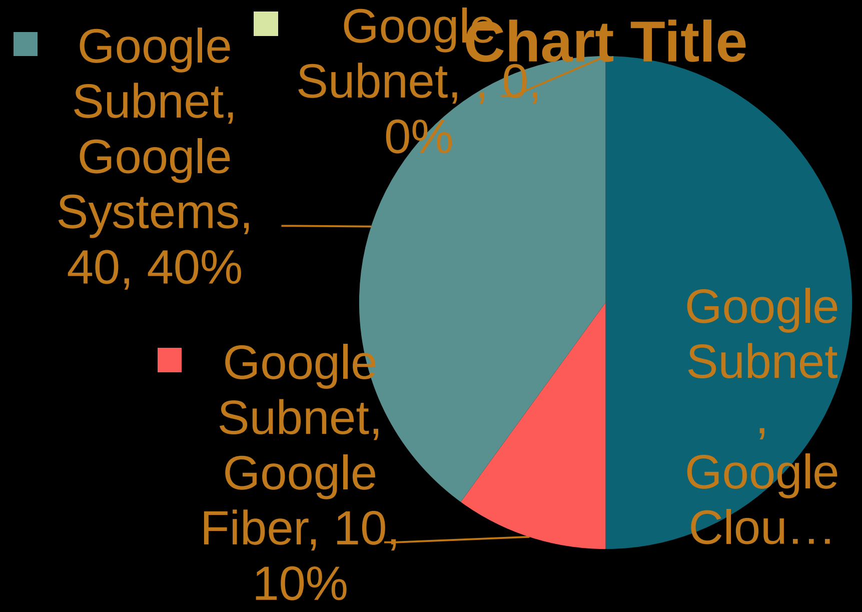


Chart Title
Google Subnet, Google Systems, 40, 40%
Google Subnet, , 0, 0%
Google Subnet, Google Fiber, 10, 10%
Google Subnet, Google Clou…

Got the sorted IP range!

What's next?

Extract individual IP and port scan with Nmap.

But....

Because...

- Still we have 2000*800 = 1600000 IP
- Nmap scan takes minimum of 1.30 seconds for each IP

Which would approx take 21 continuous days to finish scanning.

Thanks to Jason Haddix's review about "masscan" in Bug hunter's methodology 2.0

Tool	Time to run	Found
masscan masscan -p1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389,280,4567,7001,8008,9080 -iL $TARGET_LIST --max-rate 100000 -oG $TARGET_OUTPUT	11m4.164s	196
nmap	∞	zzz

Still.....

It would take 3 days to finish port scanning with Mass Scan.

So I need to find some other way to make this more faster and efficient.And finally I decided to go with Google Cloud Console.

What is Google Cloud Console?

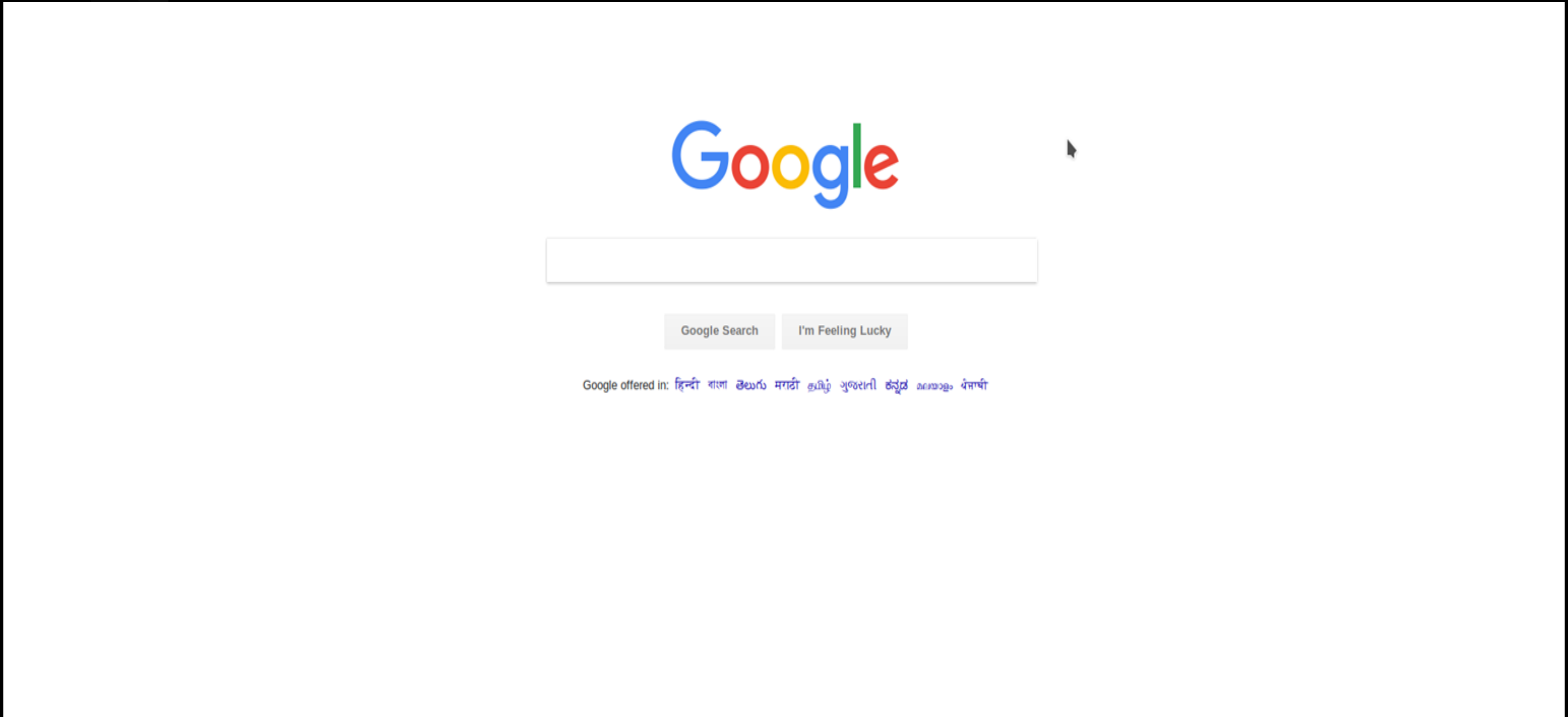
Google Cloud Console is a **FREE** VPS provided by Google. Which gives root privileges for every user. It also allow you to manage more than 2 VPS in a single account.

Ah! It's finally done..

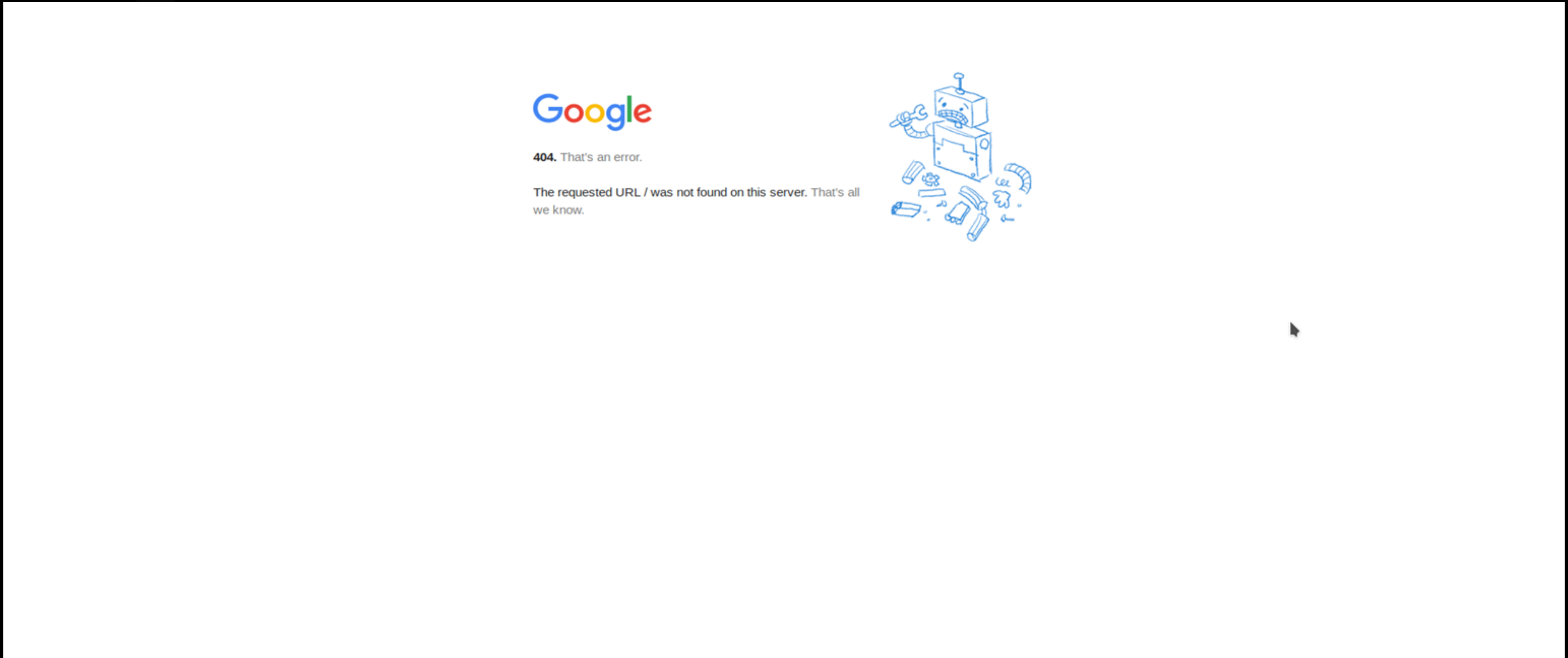
Now we have all the IP with open ports :) . **Still we have 14000 live IP to check out.**

But I was still excited to see what's on those IP. So I tried to open some of it. The sight I saw totally surprising ....

It was….this :|


Google
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ

And this!



Google

404. That's an error.

The requested URL / was not found on this server. That's all we know.

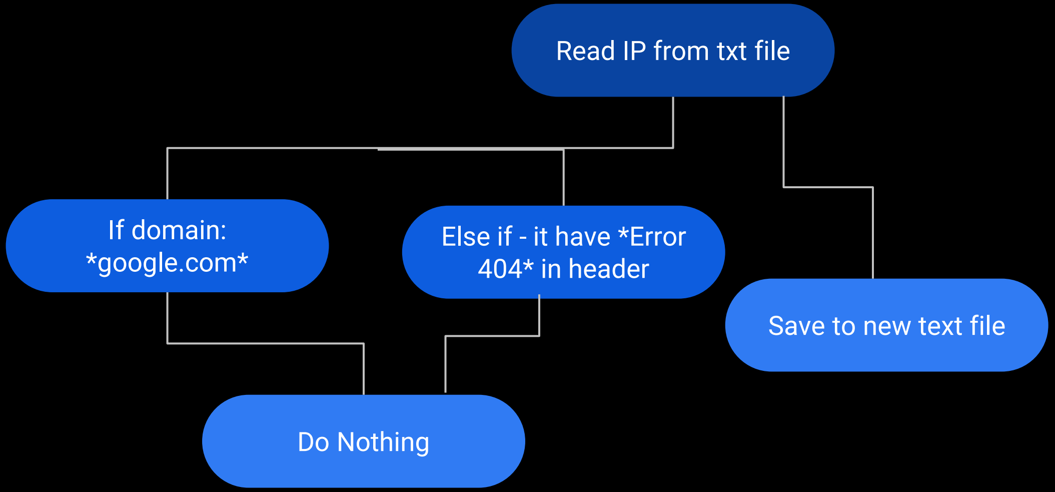
Not the time to lose hope!

There is still chance for finding at least 1 valid out of 14000 IP...So I went for that.

SORT IT AGAIN!

Then my task was to remove all those IP which are redirecting to Google.com and which are throwing out classic 404 error. Bash comes to rescue again. I made a simple bash script again which use an infamous tool called "CURL" to detect these pattern and remove those IP form the list. As the process was huge I decided to put this also in cloud.

Mass-Curl



Read IP from txt file

If domain: *google.com*

Else if - it have *Error 404* in header

Save to new text file

Do Nothing

Removed the scrap!

Now we have 5000 IP to look on! Still a big number right?

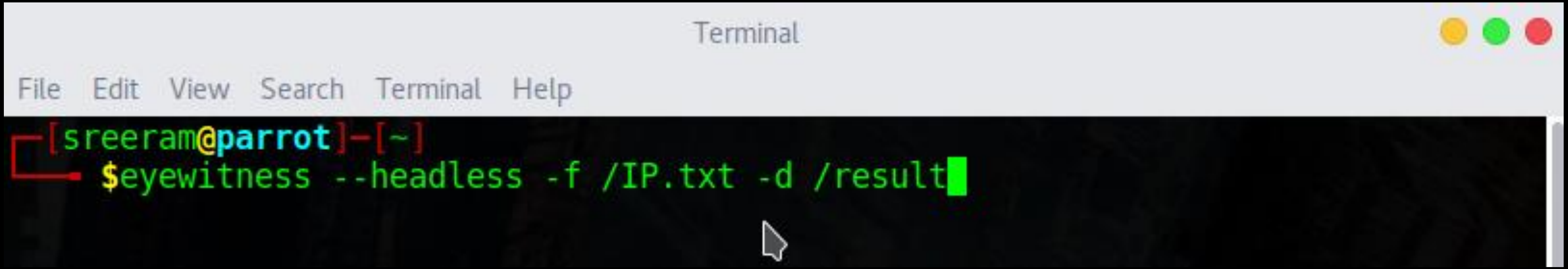
Let's automate it again!

But this time, VISUALLY!

Eyewitness...

Eyewitness is a tool made by Christopher Truncer which simply takes screenshot of the list of URL provided. It also provide report of the provided list. Which includes, header, Http response, response code and source code.

Eyewitness usage:

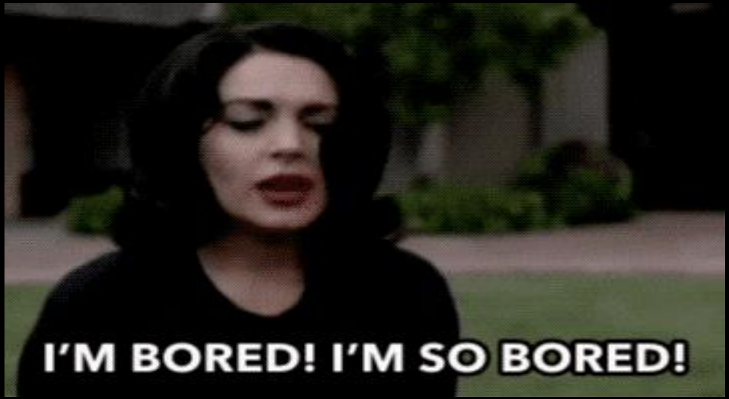


```
┌─[sreeram@parrot]─[~]
└──╼ $eyewitness --headless -f /IP.txt -d /result
```

After some days of pause and play!

The task of eyewitness was completed. Now we have a lot screenshots to lookup.

I went through one by one manually. I made note of all the fishy IP in a text file and kept on moving. Honestly...IT WAS so BOOOOOOOOOOOORING!



Now it's time for the finalist..

I got about 30 IP in my finalist list. Now let's get back into the traditional way of bug hunting. "Directory Brute-forcing". I used Dirbuster with the medium wordlist which comes default with dirbuster.

Wake Up!

Finally!

I got 2 IP with Admin Panel. And as expected one had default credentials and another didn’t even had a credentials.

1, First one was a “Youtube Streaming device”. Which is used to stream live videos over Youtube.It is also connected with Google TV network. With Admin access to this I could have played my own video on every TV in the world which uses Youtube and could have interrupted live videos from any channel .(Some kind of Watch Dogs stuffs)

2, 2nd one was titled as “Satellite Multiplex receiver/transcoder” .Yet I’m not sure what’s it. But “Satellite” sounds cool!

Reporting!

Both the bugs were reported separately. But they were merged together into one report as the root cause is same. And was rewarded $13337 for this.

The FIX:

The fix was pretty simple. Google Security team made those IP unreachable from internet and can be accessed only with a proxy, VPN or from local networks of Google.

THAT’S IT