Gurashish Anand
Final report:-

1(Public and External Vulnerabilities):-

We will start by learning about what autograph.io is, and what is their current stand.

- So , Autograph started off as an NFT platform that brings together the most iconic brands and legendary names in sports, entertainment and culture to create unique digital collections and experiences.
- After knowing that the firm deals in NFT, I checked for some updates about it on “The Crypto Times” and found out that the company is going through a pivot due to the crypto crash and trying to have a broader vision for its future.

Now that we know what the company is, let’s dig in.

Stuff found:-

1. ***WHOIS***

Using WHOIS, we tried gathering information about the DNS that might reveal potential vulnerabilities:-

WHOIS search results

Domain Name: autograph.io
Registry Domain ID: ebd1e9f612eb4cce840b9340b31f92d3-DONUTS
Registrar WHOIS Server: whois.gandi.net
Registrar URL: https://www.gandi.net
Updated Date: 2023-03-14T02:59:59Z
Creation Date: 2019-04-12T10:07:29Z
Registry Expiry Date: 2024-04-12T10:07:29Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Here:-

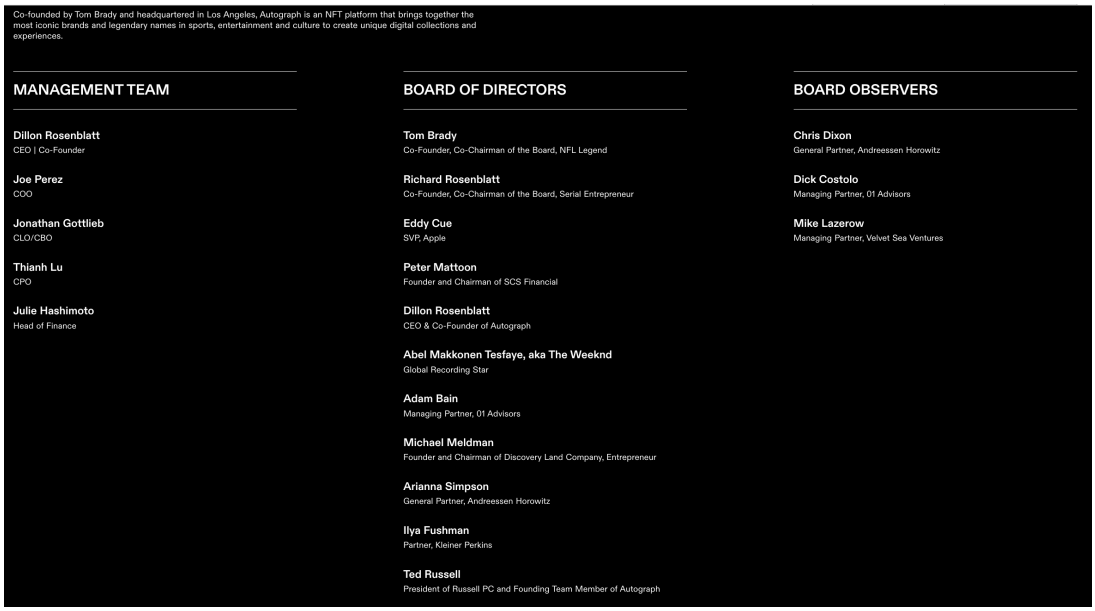
- The domain expiration date is exposed, which enables someone to

potentially be take over the website, leading to serious security issues for the original owner.

- Other information gathered from WHOIS like abuse contact details might not have a direct technical harm to autograph, but it can be used by the attacker for social engineering purposes like spear phishing.

2. ***Public information.***

If get more information about the executive board on the about page of the website, which gives attacker more information for spear phishing and whaling. The first line tells us that the company is headquartered in LA, so this information came in handy to find out the address of the headquarters.



Co-founded by Tom Brady and headquartered in Los Angeles, Autograph is an NFT platform that brings together the most iconic brands and legendary names in sports, entertainment and culture to create unique digital collections and experiences.

MANAGEMENT TEAM

Dillon Rosenblatt
CEO | Co-Founder

Joe Perez
COO

Jonathan Gottlieb
CLO/CBO

Thianh Lu
CPO

Julie Hashimoto
Head of Finance

BOARD OF DIRECTORS

Tom Brady
Co-Founder, Co-Chairman of the Board, NFL Legend

Richard Rosenblatt
Co-Founder, Co-Chairman of the Board, Serial Entrepreneur

Eddy Cue
SVP, Apple

Peter Mattoon
Founder and Chairman of SCS Financial

Dillon Rosenblatt
CEO & Co-Founder of Autograph

Abel Makkonen Tesfaye, aka The Weeknd
Global Recording Star

Adam Bain
Managing Partner, 01 Advisors

Michael Meldman
Founder and Chairman of Discovery Land Company, Entrepreneur

Arianna Simpson
General Partner, Andreessen Horowitz

Ilya Fushman
Partner, Kleiner Perkins

Ted Russell
President of Russell PC and Founding Team Member of Autograph

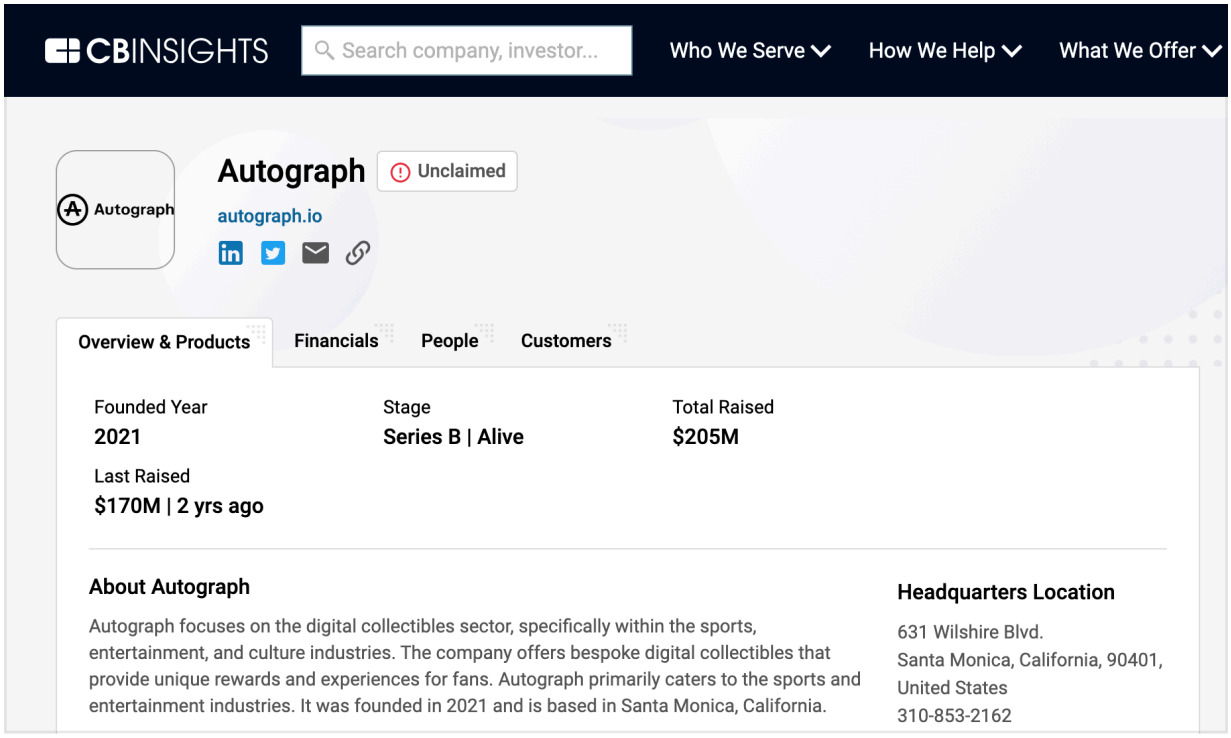
BOARD OBSERVERS

Chris Dixon
General Partner, Andreessen Horowitz

Dick Costolo
Managing Partner, 01 Advisors

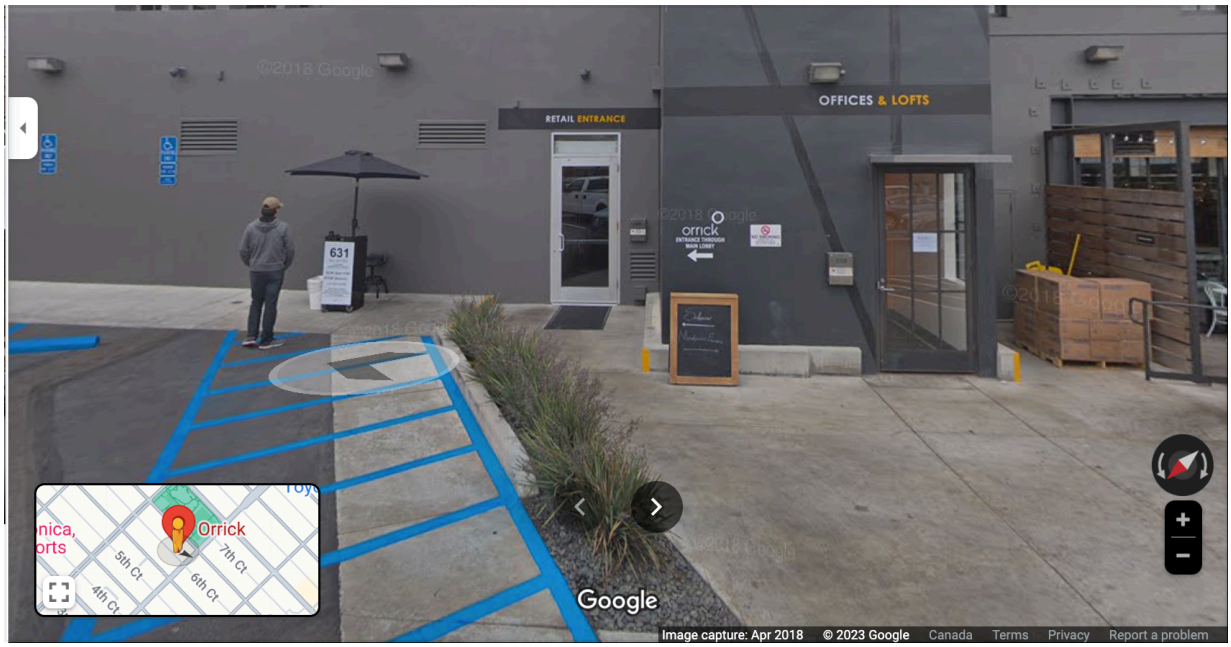
Mike Lazerow
Managing Partner, Velvet Sea Ventures

A website called ‘cbinsights.com’ was to locate the headquarters, which is at ‘631 Wilshire Blvd,Santa Monica, California, 90401,
United States’.



3.Using Google Maps to find out the physical vulnerabilities.

As we explore the google street view, we see that the building has a labelling as "OFFICES & LOFTS". This could mean that the building comprises of different offices, which would also mean that it would use the same parking lot.

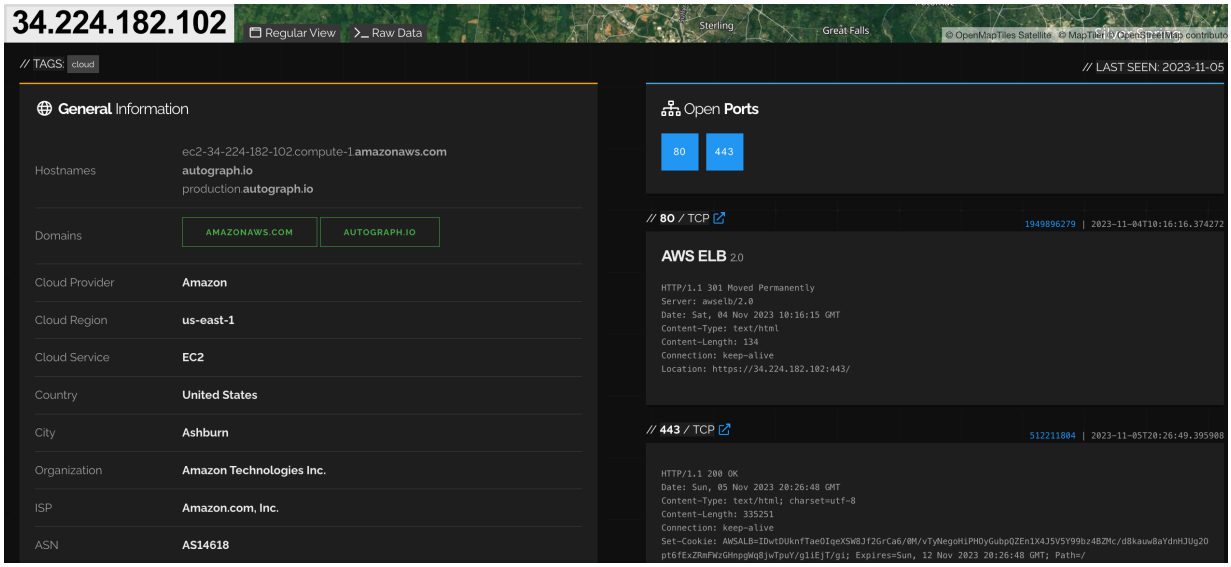


As we explore further, wee see that there are no security cameras and parking checks, so it wouldn't be wrong to say that the outer physical perimeter of the headquarters is not fully secured.

4.Shodan.

Now that we are done with our non-technical lookups, we will use Shodan to look for open ports and connected devices.

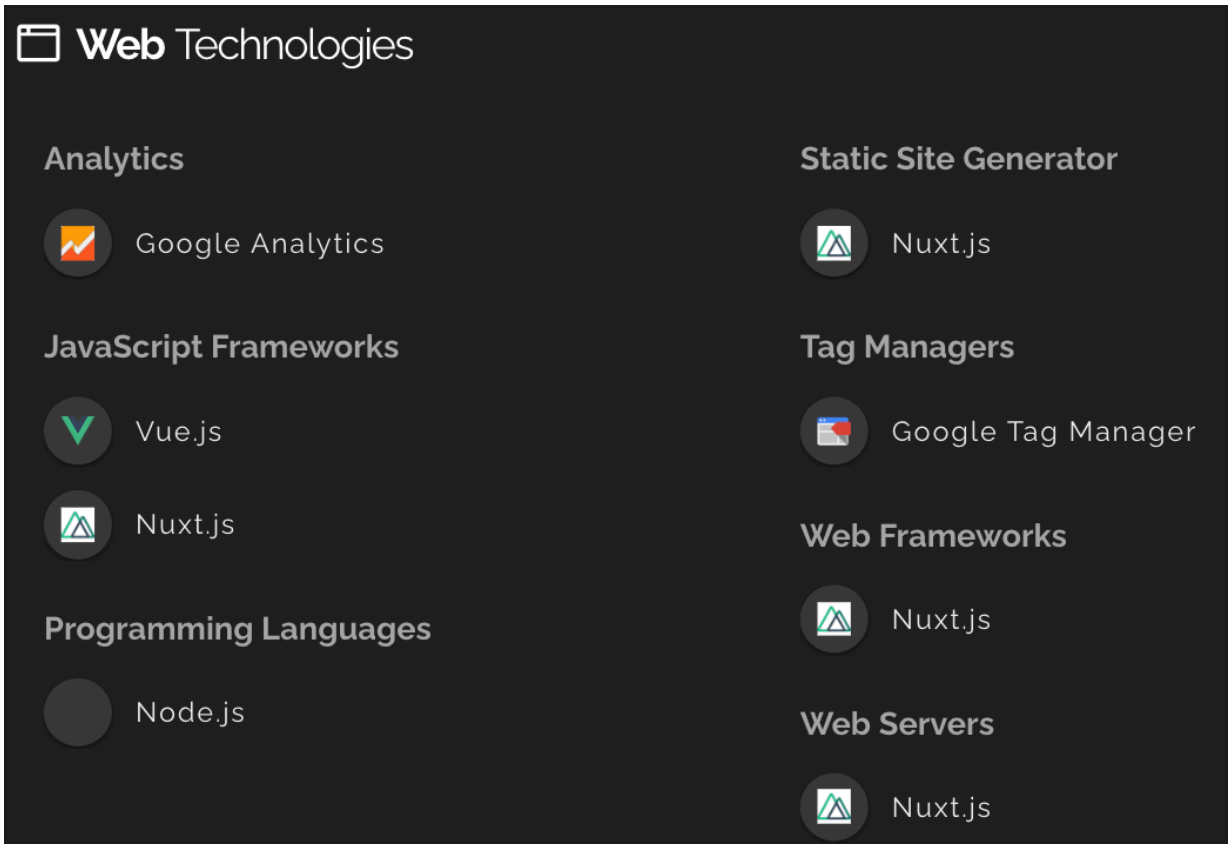
- First of all, we used the query “hostname:autograph” to find out more information, and we find out that port 80 and 443 are open, which means that the website is using HTTP and HTTPS, which is quite obvious. We also find out an IP associated with the website and the fact that the website is using AWS for its cloud processes.



- If we scroll through the port 443 results, we find out the SSL certificate’s validity. We also find out all the technologies that are used to build this website, and this information can be very useful to the red team in figuring out what exploits to use to compromise this website.

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            09:5e:ef:cd:e2:37:0e:b4:a9:34:d0:5b:0d:c6:1c:8c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Amazon, CN=Amazon RSA 2048 M02
        Validity
            Not Before: Dec 16 00:00:00 2022 GMT
            Not After : Jan 15 23:59:59 2024 GMT
        Subject: CN=production.autograph.io
```



2.(Internal Vulnerabilities)

Firstly, I made a text file with all the IP addresses provided so that I can perform a group scan using ***"NMAP"***. However, I wasn't able to do that as a lot of the hosts were probably down.

```
gurashishanand@gee Downloads % nmap -iL targets.txt

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 22:59 EST
Strange read error from 236.129.26.6 (47 - 'Address family not supported by protocol family')
Strange read error from 225.229.239.40 (47 - 'Address family not supported by protocol family')
```

So, this seemed like a time to check for all hosts that are up. Using ChatGPT, I created a bash script to ping all the hosts from the IP list.

```
#!/bin/bash

# Check if targets.txt file exists
if [ ! -f targets.txt ]; then
    echo "targets.txt file not found."
    exit 1
fi

# Read each line (assuming each line contains an IP address) and ping the IP
while IFS= read -r ip; do
    ping -c 4 "$ip"  # Change the value after -c to set the number of pings
done < targets.txt
```

Following are the ones that responded:-

- 113.61.139.65
- 189.233.48.137
- 97.104.164.77
- 34.43.135.24
- 85.1.146.186
- 1.33.102.185
- 36.80.174.222
- 116.124.83.121
- 178.116.144.99
- 4.14.112.222
- 123.135.15.161
- 117.206.65.36
- 47.33.188.38
- 118.33.172.166
- 104.119.72.137
- 60.127.252.1
- 104.168.160.196

Now that I had the list of all the hosts that are up, I'll used ***NMAP*** to scan all the hosts for ports and services.

Command used:- ***nmap -sV -sC -T4 -Pn 113.61.139.65 189.233.48.137 97.104.164.77 34.43.135.24 85.1.146.186 1.33.102.185 36.80.174.222 116.124.83.121 178.116.144.99 4.14.112.222 123.135.15.161 117.206.65.36 47.33.188.38 118.33.172.166 104.119.72.137 60.127.252.1 104.168.160.196.***

Vulnerabilities found by analyzing the nmap report:-

113.61.139.65

- Subdomain found:- 113-61-139-65.veetime.com.
- To sum up, the examined host displays multiple restricted ports typically utilized by Microsoft services. Meanwhile, it has an active port 8080 running an HTTP service linked to the T-Home Telekom Media Receiver. This device seems connected to media services and likely employs security protocols to limit access to specific ports. The host also has port 8086 is open and using a generic 'tcpwrapped' service. This often means that a service is available but not identifiable by Nmap.

189.233.48.137

- Nothing found.

97.104.164.77

- Nothing found.

34.43.135.24

- This host has the highest number of open ports, which is most of the ports from port 1 to port 65389. These ports have a service running called “tcpwrapped”, which just means that there is some service running on these ports but it’s not recognized by nmap.
- Regardless, this machine exposes several potential vulnerabilities as ports commonly associated with specific services like SSH, SMTP, MSRPC, and NetBIOS are either reported as 'filtered' or 'open' but not fully identified.

85.1.146.186

- The Nmap analysis reveals that various ports (SMTP, DNS, MSRPC, NetBIOS, Microsoft-DS, X9-ICUE, WAP-WSP, and an unidentified service) on the IP address 85.1.146.186 are filtered, indicating that Nmap couldn't ascertain their status. This usually suggests deliberate obstruction or control over these ports, perhaps for security purposes to ward off potential vulnerabilities or unauthorized entry. Additional investigation or probing is necessary to identify any particular weaknesses.

1.33.102.185

- Nothing found.

36.80.174.222

- Nothing found.

116.124.83.121

- This host just has a closed port 113 which might be an identification/ authorization service which is blocked by the host.

178.116.144.99

- This host also just has port 8080/tcp (http-proxy) which is marked as 'closed.' When a port is labeled 'closed,' it indicates that it's not currently open to incoming connections. Specifically, port 8080 is commonly associated with HTTP proxy services. The 'closed' status signifies that either no service is operational on this port, or the service is inaccessible from the scanning location due to security configurations, software settings, or the service may not be actively accepting connections.

4.14.112.222

- Nothing found.

123.135.15.161

- Nothing found.

117.206.65.36

- The Nmap analysis of the IP address 117.206.65.36 reveals numerous closed ports linked to services such as login, shell, RPC, Freeciv, and Asterix. These closed ports signal that these particular services are currently inaccessible. If these services were accidentally exposed or possessed unpatched vulnerabilities, there could be potential security risks, enabling specific exploits or unauthorized entry. Moreover, the substantial quantity of filtered ports implies stringent firewall regulations that restrict access, potentially reducing the available attack surface.

47.33.188.38

- The Nmap analysis on IP address 47.33.188.38 discovered an accessible port 5101/tcp operating a service named 'admdog'. This unidentified service raises potential vulnerabilities because of its unknown nature.

118.33.172.166

- The Nmap analysis of IP 118.33.172.166 indicates the presence of several

filtered ports (25, 80, 135, 139, 179, 445, 2869, 4444, 4662, 8899, 9000, 52869). These filtered ports imply potential vulnerabilities because of the restricted access to crucial services like SMTP, HTTP, MSRPC, and others.

104.119.72.137

- The Nmap analysis on IP 104.119.72.137 reveals active ports (80/tcp and 443/tcp) operating Akamai's HTTP Acceleration/Mirror service for Univision Communications Inc. Possible vulnerabilities are linked to an expired SSL certificate and concerns with HTTP title configurations, which could indicate URL-related issues rather than direct vulnerabilities.

60.127.252.1

- The IP scan using Nmap on IP 60.127.252.1 identified several ports (25, 80, 135, 139, 340, 445, 2103, 8000, 55555, 55600) that are filtered. This restriction of access affects crucial services like SMTP, HTTP, MSRPC, and more, which mitigates potential attacks but complicates the evaluation of specific vulnerabilities due to the lack of access to these services.

104.168.160.196

- This host exposes the highest number of vulnerabilities. The IP scan conducted by Nmap on IP address 104.168.160.196 detects several accessible ports operating services such as FTP, DNS, HTTP, and email (POP3, IMAP, SMTP), along with MySQL. Possible vulnerabilities encompass concerns about the validity of SSL certificates, service versions that may house known vulnerabilities, and potential misconfigurations in services, as evidenced by error messages. Exploiting these issues could enable attackers to gain unauthorized access or engage in malicious activities. Regular updates and appropriate configuration are crucial to address and mitigate these vulnerabilities.

Nmap report:-

gurashishanand@gee ~ % nmap -sV -sC -T4 -Pn 113.61.139.65 189.233.48.137 97.104.164.77 34.43.135.24 85.1.146.186 1.33.102.185 36.80.174.222 116.124.83.121 178.116.144.99 4.14.112.222 123.135.15.161 117.206.65.36 47.33.188.38 118.33.172.166 104.119.72.137 60.127.252.1 104.168.160.196

Starting Nmap 7.94 (https://nmap.org) at 2023-11-06 00:43 EST
Warning: 60.127.252.1 giving up on port because retransmission cap hit (6).
Nmap scan report for 113-61-139-65.veetime.com (113.61.139.65)
Host is up (0.25s latency).

Not shown: 994 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
25/tcp filtered smtp
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
8080/tcp open http T-Home Telekom Media Receiver httpd
|_http-title: Site doesn't have a title.
8086/tcp open tcpwrapped
Service Info: Device: media device

Nmap scan report for dsl-189-233-48-137-dyn.prod-infinitum.com.mx (189.233.48.137)
Host is up.
All 1000 scanned ports on dsl-189-233-48-137-dyn.prod-infinitum.com.mx (189.233.48.137) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 097-104-164-077.res.spectrum.com (97.104.164.77)
Host is up.
All 1000 scanned ports on 097-104-164-077.res.spectrum.com (97.104.164.77) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 24.135.43.34.bc.googleusercontent.com (34.43.135.24)
Host is up (0.033s latency).

Bug in uptime-agent-info: no string output.
PORT STATE SERVICE VERSION
1/tcp open tcpwrapped
3/tcp open tcpwrapped
4/tcp open tcpwrapped
6/tcp open tcpwrapped
7/tcp open tcpwrapped
9/tcp open tcpwrapped
13/tcp open tcpwrapped
17/tcp open tcpwrapped
19/tcp open tcpwrapped
20/tcp open tcpwrapped
21/tcp open tcpwrapped
22/tcp open tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
23/tcp open tcpwrapped
24/tcp open tcpwrapped

25/tcp filtered smtp
26/tcp open tcpwrapped
30/tcp open tcpwrapped
32/tcp open tcpwrapped
33/tcp open tcpwrapped
37/tcp open tcpwrapped
42/tcp open tcpwrapped
43/tcp open tcpwrapped
49/tcp open tcpwrapped
53/tcp open tcpwrapped
70/tcp open tcpwrapped
|_gopher-ls:
79/tcp open tcpwrapped
80/tcp open tcpwrapped
81/tcp open tcpwrapped
82/tcp open tcpwrapped
83/tcp open tcpwrapped
84/tcp open tcpwrapped
85/tcp open tcpwrapped
88/tcp open tcpwrapped
89/tcp open tcpwrapped
90/tcp open tcpwrapped
99/tcp open tcpwrapped
100/tcp open tcpwrapped
106/tcp open tcpwrapped
109/tcp open tcpwrapped
110/tcp open tcpwrapped
111/tcp open tcpwrapped
113/tcp open tcpwrapped
119/tcp open tcpwrapped
125/tcp open tcpwrapped
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
143/tcp open tcpwrapped
144/tcp open tcpwrapped
146/tcp open tcpwrapped
161/tcp open tcpwrapped
163/tcp open tcpwrapped
179/tcp open tcpwrapped
199/tcp open tcpwrapped
211/tcp open tcpwrapped
212/tcp open tcpwrapped
222/tcp open tcpwrapped
254/tcp open tcpwrapped

255/tcp   open   tcpwrapped
256/tcp   open   tcpwrapped
259/tcp   open   tcpwrapped
264/tcp   open   tcpwrapped
280/tcp   open   tcpwrapped
301/tcp   open   tcpwrapped
306/tcp   open   tcpwrapped
311/tcp   open   tcpwrapped
340/tcp   open   tcpwrapped
366/tcp   open   tcpwrapped
389/tcp   open   tcpwrapped
406/tcp   open   tcpwrapped
407/tcp   open   tcpwrapped
416/tcp   open   tcpwrapped
417/tcp   open   tcpwrapped
425/tcp   open   tcpwrapped
427/tcp   open   tcpwrapped
443/tcp   open   tcpwrapped
444/tcp   open   tcpwrapped
445/tcp   filtered microsoft-ds
458/tcp   open   tcpwrapped
464/tcp   open   tcpwrapped
465/tcp   open   tcpwrapped
|_smtp-commands: Couldn't establish connection on port 465
481/tcp   open   tcpwrapped
497/tcp   open   tcpwrapped
500/tcp   open   tcpwrapped
512/tcp   open   tcpwrapped
513/tcp   open   tcpwrapped
514/tcp   open   tcpwrapped
515/tcp   open   tcpwrapped
524/tcp   open   tcpwrapped
541/tcp   open   tcpwrapped
543/tcp   open   tcpwrapped
544/tcp   open   tcpwrapped
545/tcp   open   tcpwrapped
548/tcp   open   tcpwrapped
|_afp-serverinfo: ERROR: Script execution failed (use -d to debug)
554/tcp   open   tcpwrapped
555/tcp   open   tcpwrapped
563/tcp   open   tcpwrapped
587/tcp   open   tcpwrapped
|_smtp-commands: Couldn't establish connection on port 587
593/tcp   open   tcpwrapped

616/tcp open tcpwrapped
617/tcp open tcpwrapped
625/tcp open tcpwrapped
631/tcp open tcpwrapped
636/tcp open tcpwrapped
646/tcp open tcpwrapped
648/tcp open tcpwrapped
666/tcp open tcpwrapped
667/tcp open tcpwrapped
668/tcp open tcpwrapped
683/tcp open tcpwrapped
687/tcp open tcpwrapped
691/tcp open tcpwrapped
700/tcp open tcpwrapped
705/tcp open tcpwrapped
711/tcp open tcpwrapped
714/tcp open tcpwrapped
720/tcp open tcpwrapped
722/tcp open tcpwrapped
726/tcp open tcpwrapped
749/tcp open tcpwrapped
765/tcp open tcpwrapped
777/tcp open tcpwrapped
783/tcp open tcpwrapped
787/tcp open tcpwrapped
800/tcp open tcpwrapped
801/tcp open tcpwrapped
808/tcp open tcpwrapped
843/tcp open tcpwrapped
873/tcp open tcpwrapped
880/tcp open tcpwrapped
888/tcp open tcpwrapped
898/tcp open tcpwrapped
900/tcp open tcpwrapped
901/tcp open tcpwrapped
902/tcp open tcpwrapped
903/tcp open tcpwrapped
911/tcp open tcpwrapped
912/tcp open tcpwrapped
981/tcp open tcpwrapped
987/tcp open tcpwrapped
990/tcp open tcpwrapped
992/tcp open tcpwrapped
993/tcp open tcpwrapped

995/tcp open tcpwrapped
999/tcp open tcpwrapped
1000/tcp open tcpwrapped
1001/tcp open tcpwrapped
1002/tcp open tcpwrapped
1007/tcp open tcpwrapped
1009/tcp open tcpwrapped
1010/tcp open tcpwrapped
1011/tcp open tcpwrapped
1021/tcp open tcpwrapped
1022/tcp open tcpwrapped
1023/tcp open tcpwrapped
1024/tcp open tcpwrapped
1025/tcp open tcpwrapped
1026/tcp open tcpwrapped
1027/tcp open tcpwrapped
1028/tcp open tcpwrapped
1029/tcp open tcpwrapped
1030/tcp open tcpwrapped
1031/tcp open tcpwrapped
1032/tcp open tcpwrapped
1033/tcp open tcpwrapped
1034/tcp open tcpwrapped
1035/tcp open tcpwrapped
1036/tcp open tcpwrapped
1037/tcp open tcpwrapped
1038/tcp open tcpwrapped
1039/tcp open tcpwrapped
1040/tcp open tcpwrapped
1041/tcp open tcpwrapped
1042/tcp open tcpwrapped
1043/tcp open tcpwrapped
1044/tcp open tcpwrapped
1045/tcp open tcpwrapped
1046/tcp open tcpwrapped
1047/tcp open tcpwrapped
1048/tcp open tcpwrapped
1049/tcp open tcpwrapped
1050/tcp open tcpwrapped
1051/tcp open tcpwrapped
1052/tcp open tcpwrapped
1053/tcp open tcpwrapped
1054/tcp open tcpwrapped
1055/tcp open tcpwrapped

1056/tcp open tcpwrapped
1057/tcp open tcpwrapped
1058/tcp open tcpwrapped
1059/tcp open tcpwrapped
1060/tcp open tcpwrapped
1061/tcp open tcpwrapped
1062/tcp open tcpwrapped
1063/tcp open tcpwrapped
1064/tcp open tcpwrapped
1065/tcp open tcpwrapped
1066/tcp open tcpwrapped
1067/tcp open tcpwrapped
1068/tcp open tcpwrapped
1069/tcp open tcpwrapped
1070/tcp open tcpwrapped
1071/tcp open tcpwrapped
1072/tcp open tcpwrapped
1073/tcp open tcpwrapped
1074/tcp open tcpwrapped
1075/tcp open tcpwrapped
1076/tcp open tcpwrapped
1077/tcp open tcpwrapped
1078/tcp open tcpwrapped
1079/tcp open tcpwrapped
1080/tcp open tcpwrapped
1081/tcp open tcpwrapped
1082/tcp open tcpwrapped
1083/tcp open tcpwrapped
1084/tcp open tcpwrapped
1085/tcp open tcpwrapped
1086/tcp open tcpwrapped
1087/tcp open tcpwrapped
1088/tcp open tcpwrapped
1089/tcp open tcpwrapped
1090/tcp open tcpwrapped
1091/tcp open tcpwrapped
1092/tcp open tcpwrapped
1093/tcp open tcpwrapped
1094/tcp open tcpwrapped
1095/tcp open tcpwrapped
1096/tcp open tcpwrapped
1097/tcp open tcpwrapped
1098/tcp open tcpwrapped
1099/tcp open tcpwrapped

1100/tcp open tcpwrapped
1102/tcp open tcpwrapped
1104/tcp open tcpwrapped
1105/tcp open tcpwrapped
1106/tcp open tcpwrapped
1107/tcp open tcpwrapped
1108/tcp open tcpwrapped
1110/tcp open tcpwrapped
1111/tcp open tcpwrapped
1112/tcp open tcpwrapped
1113/tcp open tcpwrapped
1114/tcp open tcpwrapped
1117/tcp open tcpwrapped
1119/tcp open tcpwrapped
1121/tcp open tcpwrapped
1122/tcp open tcpwrapped
1123/tcp open tcpwrapped
1124/tcp open tcpwrapped
1126/tcp open tcpwrapped
1130/tcp open tcpwrapped
1131/tcp open tcpwrapped
1132/tcp open tcpwrapped
1137/tcp open tcpwrapped
1138/tcp open tcpwrapped
1141/tcp open tcpwrapped
1145/tcp open tcpwrapped
1147/tcp open tcpwrapped
1148/tcp open tcpwrapped
1149/tcp open tcpwrapped
1151/tcp open tcpwrapped
1152/tcp open tcpwrapped
1154/tcp open tcpwrapped
1163/tcp open tcpwrapped
1164/tcp open tcpwrapped
1165/tcp open tcpwrapped
1166/tcp open tcpwrapped
1169/tcp open tcpwrapped
1174/tcp open tcpwrapped
1175/tcp open tcpwrapped
1183/tcp open tcpwrapped
1185/tcp open tcpwrapped
1186/tcp open tcpwrapped
1187/tcp open tcpwrapped
1192/tcp open tcpwrapped

1198/tcp open tcpwrapped
1199/tcp open tcpwrapped
1201/tcp open tcpwrapped
1213/tcp open tcpwrapped
1216/tcp open tcpwrapped
1217/tcp open tcpwrapped
1218/tcp open tcpwrapped
1233/tcp open tcpwrapped
1234/tcp open tcpwrapped
1236/tcp open tcpwrapped
1244/tcp open tcpwrapped
1247/tcp open tcpwrapped
1248/tcp open tcpwrapped
1259/tcp open tcpwrapped
1271/tcp open tcpwrapped
1272/tcp open tcpwrapped
1277/tcp open tcpwrapped
1287/tcp open tcpwrapped
1296/tcp open tcpwrapped
1300/tcp open tcpwrapped
1301/tcp open tcpwrapped
1309/tcp open tcpwrapped
1310/tcp open tcpwrapped
1311/tcp open tcpwrapped
1322/tcp open tcpwrapped
1328/tcp open tcpwrapped
1334/tcp open tcpwrapped
1352/tcp open tcpwrapped
1417/tcp open tcpwrapped
1433/tcp open tcpwrapped
1434/tcp open tcpwrapped
1443/tcp open tcpwrapped
1455/tcp open tcpwrapped
1461/tcp open tcpwrapped
1494/tcp open tcpwrapped
1500/tcp open tcpwrapped
1501/tcp open tcpwrapped
1503/tcp open tcpwrapped
1521/tcp open tcpwrapped
1524/tcp open tcpwrapped
1533/tcp open tcpwrapped
1556/tcp open tcpwrapped
1580/tcp open tcpwrapped
1583/tcp open tcpwrapped

1594/tcp open tcpwrapped
1600/tcp open tcpwrapped
1641/tcp open tcpwrapped
1658/tcp open tcpwrapped
1666/tcp open tcpwrapped
1687/tcp open tcpwrapped
1688/tcp open tcpwrapped
1700/tcp open tcpwrapped
1717/tcp open tcpwrapped
1718/tcp open tcpwrapped
1719/tcp open tcpwrapped
1720/tcp open tcpwrapped
1721/tcp open tcpwrapped
1723/tcp open tcpwrapped
1755/tcp open tcpwrapped
1761/tcp open tcpwrapped
1782/tcp open tcpwrapped
1783/tcp open tcpwrapped
1801/tcp open tcpwrapped
1805/tcp open tcpwrapped
1812/tcp open tcpwrapped
1839/tcp open tcpwrapped
1840/tcp open tcpwrapped
1862/tcp open tcpwrapped
1863/tcp open tcpwrapped
1864/tcp open tcpwrapped
1875/tcp open tcpwrapped
1900/tcp open tcpwrapped
1914/tcp open tcpwrapped
1935/tcp open tcpwrapped
1947/tcp open tcpwrapped
1971/tcp open tcpwrapped
1972/tcp open tcpwrapped
1974/tcp open tcpwrapped
1984/tcp open tcpwrapped
1998/tcp open tcpwrapped
1999/tcp open tcpwrapped
2000/tcp open tcpwrapped
2001/tcp open tcpwrapped
2002/tcp open tcpwrapped
2003/tcp open tcpwrapped
2004/tcp open tcpwrapped
2005/tcp open tcpwrapped
2006/tcp open tcpwrapped

2007/tcp open tcpwrapped
2008/tcp open tcpwrapped
2009/tcp open tcpwrapped
2010/tcp open tcpwrapped
2013/tcp open tcpwrapped
2020/tcp open tcpwrapped
2021/tcp open tcpwrapped
2022/tcp open tcpwrapped
2030/tcp open tcpwrapped
2033/tcp open tcpwrapped
2034/tcp open tcpwrapped
2035/tcp open tcpwrapped
2038/tcp open tcpwrapped
2040/tcp open tcpwrapped
2041/tcp open tcpwrapped
2042/tcp open tcpwrapped
2043/tcp open tcpwrapped
2045/tcp open tcpwrapped
2046/tcp open tcpwrapped
2047/tcp open tcpwrapped
2048/tcp open tcpwrapped
2049/tcp open tcpwrapped
2065/tcp open tcpwrapped
2068/tcp open tcpwrapped
2099/tcp open tcpwrapped
2100/tcp open tcpwrapped
2103/tcp open tcpwrapped
2105/tcp open tcpwrapped
2106/tcp open tcpwrapped
2107/tcp open tcpwrapped
2111/tcp open tcpwrapped
2119/tcp open tcpwrapped
2121/tcp open tcpwrapped
2126/tcp open tcpwrapped
2135/tcp open tcpwrapped
2144/tcp open tcpwrapped
2160/tcp open tcpwrapped
2161/tcp open tcpwrapped
2170/tcp open tcpwrapped
2179/tcp open tcpwrapped
2190/tcp open tcpwrapped
2191/tcp open tcpwrapped
2196/tcp open tcpwrapped
2200/tcp open tcpwrapped

2222/tcp open   tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
2251/tcp open   tcpwrapped
2260/tcp open   tcpwrapped
2288/tcp open   tcpwrapped
2301/tcp open   tcpwrapped
2323/tcp open   tcpwrapped
2366/tcp open   tcpwrapped
2381/tcp open   tcpwrapped
2382/tcp open   tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
2383/tcp open   tcpwrapped
2393/tcp open   tcpwrapped
2394/tcp open   tcpwrapped
2399/tcp open   tcpwrapped
2401/tcp open   tcpwrapped
2492/tcp open   tcpwrapped
2500/tcp open   tcpwrapped
2522/tcp open   tcpwrapped
2525/tcp open   tcpwrapped
2557/tcp open   tcpwrapped
2601/tcp open   tcpwrapped
2602/tcp open   tcpwrapped
2604/tcp open   tcpwrapped
2605/tcp open   tcpwrapped
2607/tcp open   tcpwrapped
2608/tcp open   tcpwrapped
2638/tcp open   tcpwrapped
2701/tcp open   tcpwrapped
2702/tcp open   tcpwrapped
2710/tcp open   tcpwrapped
2717/tcp open   tcpwrapped
2718/tcp open   tcpwrapped
2725/tcp open   tcpwrapped
2800/tcp open   tcpwrapped
2809/tcp open   tcpwrapped
2811/tcp open   tcpwrapped
2869/tcp open   tcpwrapped
2875/tcp open   tcpwrapped
2909/tcp open   tcpwrapped
2910/tcp open   tcpwrapped
2920/tcp open   tcpwrapped
2967/tcp open   tcpwrapped
2968/tcp open   tcpwrapped

2998/tcp open tcpwrapped
3000/tcp open tcpwrapped
3001/tcp open tcpwrapped
3003/tcp open tcpwrapped
3005/tcp open tcpwrapped
3006/tcp open tcpwrapped
3007/tcp open tcpwrapped
3011/tcp open tcpwrapped
3013/tcp open tcpwrapped
3017/tcp open tcpwrapped
3030/tcp open tcpwrapped
3031/tcp open tcpwrapped
3052/tcp open tcpwrapped
3071/tcp open tcpwrapped
3077/tcp open tcpwrapped
3128/tcp open tcpwrapped
3168/tcp open tcpwrapped
3211/tcp open tcpwrapped
3221/tcp open tcpwrapped
3260/tcp open tcpwrapped
3261/tcp open tcpwrapped
3268/tcp open tcpwrapped
3269/tcp open tcpwrapped
3283/tcp open tcpwrapped
3300/tcp open tcpwrapped
3301/tcp open tcpwrapped
3306/tcp open tcpwrapped
3322/tcp open tcpwrapped
3323/tcp open tcpwrapped
3324/tcp open tcpwrapped
3325/tcp open tcpwrapped
3333/tcp open tcpwrapped
3351/tcp open tcpwrapped
3367/tcp open tcpwrapped
3369/tcp open tcpwrapped
3370/tcp open tcpwrapped
3371/tcp open tcpwrapped
3372/tcp open tcpwrapped
3389/tcp open tcpwrapped
3390/tcp open tcpwrapped
3404/tcp open tcpwrapped
3476/tcp open tcpwrapped
3493/tcp open tcpwrapped
3517/tcp open tcpwrapped

3527/tcp open tcpwrapped
3546/tcp open tcpwrapped
3551/tcp open tcpwrapped
3580/tcp open tcpwrapped
3659/tcp open tcpwrapped
3689/tcp open tcpwrapped
3690/tcp open tcpwrapped
3703/tcp open tcpwrapped
3737/tcp open tcpwrapped
3766/tcp open tcpwrapped
3784/tcp open tcpwrapped
3800/tcp open tcpwrapped
3801/tcp open tcpwrapped
3809/tcp open tcpwrapped
3814/tcp open tcpwrapped
3826/tcp open tcpwrapped
3827/tcp open tcpwrapped
3828/tcp open tcpwrapped
3851/tcp open tcpwrapped
3869/tcp open tcpwrapped
3871/tcp open tcpwrapped
3878/tcp open tcpwrapped
3880/tcp open tcpwrapped
3889/tcp open tcpwrapped
3905/tcp open tcpwrapped
3914/tcp open tcpwrapped
3918/tcp open tcpwrapped
3920/tcp open tcpwrapped
3945/tcp open tcpwrapped
3971/tcp open tcpwrapped
3986/tcp open tcpwrapped
3995/tcp open tcpwrapped
3998/tcp open tcpwrapped
4000/tcp open tcpwrapped
4001/tcp open tcpwrapped
4002/tcp open tcpwrapped
4003/tcp open tcpwrapped
4004/tcp open tcpwrapped
4005/tcp open tcpwrapped
4006/tcp open tcpwrapped
4045/tcp open tcpwrapped
4111/tcp open tcpwrapped
4125/tcp open tcpwrapped
4126/tcp open tcpwrapped

4129/tcp open   tcpwrapped
4224/tcp open   tcpwrapped
4242/tcp open   tcpwrapped
|_dicom-ping: ERROR: Script execution failed (use -d to debug)
4279/tcp open   tcpwrapped
4321/tcp open   tcpwrapped
4343/tcp open   tcpwrapped
4443/tcp open   tcpwrapped
4444/tcp open   tcpwrapped
4445/tcp open   tcpwrapped
4446/tcp open   tcpwrapped
4449/tcp open   tcpwrapped
4550/tcp open   tcpwrapped
4567/tcp open   tcpwrapped
4662/tcp open   tcpwrapped
4848/tcp open   tcpwrapped
4899/tcp open   tcpwrapped
4900/tcp open   tcpwrapped
4998/tcp open   tcpwrapped
5000/tcp open   tcpwrapped
5001/tcp open   tcpwrapped
5002/tcp open   tcpwrapped
5003/tcp open   tcpwrapped
5004/tcp open   tcpwrapped
5009/tcp open   tcpwrapped
5030/tcp open   tcpwrapped
5033/tcp open   tcpwrapped
5050/tcp open   tcpwrapped
5051/tcp open   tcpwrapped
5054/tcp open   tcpwrapped
5060/tcp open   tcpwrapped
5061/tcp open   tcpwrapped
5080/tcp open   tcpwrapped
5087/tcp open   tcpwrapped
5100/tcp open   tcpwrapped
5101/tcp open   tcpwrapped
5102/tcp open   tcpwrapped
5120/tcp open   tcpwrapped
5190/tcp open   tcpwrapped
5200/tcp open   tcpwrapped
5214/tcp open   tcpwrapped
5221/tcp open   tcpwrapped
5222/tcp open   tcpwrapped
| xmpp-info:

| STARTTLS Failed
| info:
| errors:
| (timeout)
| capabilities:
| xmpp:
| auth_mechanisms:
| unknown:
| compression_methods:
|_   features:
5225/tcp open   tcpwrapped
5226/tcp open   tcpwrapped
5269/tcp open   tcpwrapped
| xmpp-info:
| STARTTLS Failed
| info:
| errors:
| (timeout)
| capabilities:
| xmpp:
| auth_mechanisms:
| unknown:
| compression_methods:
|_   features:
5280/tcp open   tcpwrapped
5298/tcp open   tcpwrapped
5357/tcp open   tcpwrapped
5405/tcp open   tcpwrapped
5414/tcp open   tcpwrapped
5431/tcp open   tcpwrapped
5432/tcp open   tcpwrapped
5440/tcp open   tcpwrapped
5500/tcp open   tcpwrapped
5510/tcp open   tcpwrapped
5544/tcp open   tcpwrapped
5550/tcp open   tcpwrapped
5555/tcp open   tcpwrapped
5560/tcp open   tcpwrapped
5566/tcp open   tcpwrapped
5631/tcp open   tcpwrapped
5633/tcp open   tcpwrapped
5666/tcp open   tcpwrapped
5678/tcp open   tcpwrapped
5679/tcp open   tcpwrapped

5718/tcp open tcpwrapped
5730/tcp open tcpwrapped
5800/tcp open tcpwrapped
5801/tcp open tcpwrapped
5802/tcp open tcpwrapped
5810/tcp open tcpwrapped
5811/tcp open tcpwrapped
5815/tcp open tcpwrapped
5822/tcp open tcpwrapped
5825/tcp open tcpwrapped
5850/tcp open tcpwrapped
5859/tcp open tcpwrapped
5862/tcp open tcpwrapped
5877/tcp open tcpwrapped
5900/tcp open tcpwrapped
5901/tcp open tcpwrapped
5902/tcp open tcpwrapped
5903/tcp open tcpwrapped
5904/tcp open tcpwrapped
5906/tcp open tcpwrapped
5907/tcp open tcpwrapped
5910/tcp open tcpwrapped
5911/tcp open tcpwrapped
5915/tcp open tcpwrapped
5922/tcp open tcpwrapped
5925/tcp open tcpwrapped
5950/tcp open tcpwrapped
5952/tcp open tcpwrapped
5959/tcp open tcpwrapped
5960/tcp open tcpwrapped
5961/tcp open tcpwrapped
5962/tcp open tcpwrapped
5963/tcp open tcpwrapped
5987/tcp open tcpwrapped
5988/tcp open tcpwrapped
5989/tcp open tcpwrapped
5998/tcp open tcpwrapped
5999/tcp open tcpwrapped
6000/tcp open tcpwrapped
6001/tcp open tcpwrapped
6002/tcp open tcpwrapped
6003/tcp open tcpwrapped
6004/tcp open tcpwrapped
6005/tcp open tcpwrapped

6006/tcp open   tcpwrapped
6007/tcp open   tcpwrapped
6009/tcp open   tcpwrapped
6025/tcp open   tcpwrapped
6059/tcp open   tcpwrapped
6100/tcp open   tcpwrapped
6101/tcp open   tcpwrapped
6106/tcp open   tcpwrapped
6112/tcp open   tcpwrapped
6123/tcp open   tcpwrapped
6129/tcp open   tcpwrapped
6156/tcp open   tcpwrapped
6346/tcp open   tcpwrapped
6389/tcp open   tcpwrapped
6502/tcp open   tcpwrapped
6510/tcp open   tcpwrapped
6543/tcp open   tcpwrapped
6547/tcp open   tcpwrapped
6565/tcp open   tcpwrapped
6566/tcp open   tcpwrapped
6567/tcp open   tcpwrapped
6580/tcp open   tcpwrapped
6646/tcp open   tcpwrapped
6666/tcp open   tcpwrapped
|_irc-info: Unable to open connection
6667/tcp open   tcpwrapped
|_irc-info: Unable to open connection
6668/tcp open   tcpwrapped
|_irc-info: Unable to open connection
6669/tcp open   tcpwrapped
|_irc-info: Unable to open connection
6689/tcp open   tcpwrapped
6692/tcp open   tcpwrapped
6699/tcp open   tcpwrapped
6779/tcp open   tcpwrapped
6788/tcp open   tcpwrapped
6789/tcp open   tcpwrapped
6792/tcp open   tcpwrapped
6839/tcp open   tcpwrapped
6881/tcp open   tcpwrapped
6901/tcp open   tcpwrapped
6969/tcp open   tcpwrapped
7000/tcp open   tcpwrapped
|_irc-info: Unable to open connection

7001/tcp open   tcpwrapped
7002/tcp open   tcpwrapped
7004/tcp open   tcpwrapped
7007/tcp open   tcpwrapped
7019/tcp open   tcpwrapped
7025/tcp open   tcpwrapped
7070/tcp open   tcpwrapped
7100/tcp open   tcpwrapped
7103/tcp open   tcpwrapped
7106/tcp open   tcpwrapped
7200/tcp open   tcpwrapped
7201/tcp open   tcpwrapped
7402/tcp open   tcpwrapped
7435/tcp open   tcpwrapped
7443/tcp open   tcpwrapped
7496/tcp open   tcpwrapped
7512/tcp open   tcpwrapped
7625/tcp open   tcpwrapped
7627/tcp open   tcpwrapped
7676/tcp open   tcpwrapped
7741/tcp open   tcpwrapped
7777/tcp open   tcpwrapped
7778/tcp open   tcpwrapped
7800/tcp open   tcpwrapped
7911/tcp open   tcpwrapped
7920/tcp open   tcpwrapped
7921/tcp open   tcpwrapped
7937/tcp open   tcpwrapped
7938/tcp open   tcpwrapped
7999/tcp open   tcpwrapped
8000/tcp open   tcpwrapped
8001/tcp open   tcpwrapped
8002/tcp open   tcpwrapped
8007/tcp open   tcpwrapped
8008/tcp open   tcpwrapped
8009/tcp open   tcpwrapped
|_ajp-methods: Failed to get a valid response for the OPTION request
8010/tcp open   tcpwrapped
8011/tcp open   tcpwrapped
8021/tcp open   tcpwrapped
8022/tcp open   tcpwrapped
8031/tcp open   tcpwrapped
8042/tcp open   tcpwrapped
8045/tcp open   tcpwrapped

8080/tcp open tcpwrapped
8081/tcp open tcpwrapped
8082/tcp open tcpwrapped
8083/tcp open tcpwrapped
8084/tcp open tcpwrapped
8085/tcp open tcpwrapped
8086/tcp open tcpwrapped
8087/tcp open tcpwrapped
8088/tcp open tcpwrapped
8089/tcp open tcpwrapped
8090/tcp open tcpwrapped
8093/tcp open tcpwrapped
8099/tcp open tcpwrapped
8100/tcp open tcpwrapped
8180/tcp open tcpwrapped
8181/tcp open tcpwrapped
8192/tcp open tcpwrapped
8193/tcp open tcpwrapped
8194/tcp open tcpwrapped
8200/tcp open tcpwrapped
8222/tcp open tcpwrapped
8254/tcp open tcpwrapped
8290/tcp open tcpwrapped
8291/tcp open tcpwrapped
8292/tcp open tcpwrapped
8300/tcp open tcpwrapped
8333/tcp open tcpwrapped
8383/tcp open tcpwrapped
8400/tcp open tcpwrapped
8402/tcp open tcpwrapped
8443/tcp open tcpwrapped
8500/tcp open tcpwrapped
8600/tcp open tcpwrapped
8649/tcp open tcpwrapped
8651/tcp open tcpwrapped
8652/tcp open tcpwrapped
8654/tcp open tcpwrapped
8701/tcp open tcpwrapped
8800/tcp open tcpwrapped
8873/tcp open tcpwrapped
8888/tcp open tcpwrapped
8899/tcp open tcpwrapped
8994/tcp open tcpwrapped
9000/tcp open tcpwrapped

9001/tcp open tcpwrapped
9002/tcp open tcpwrapped
9003/tcp open tcpwrapped
9009/tcp open tcpwrapped
9010/tcp open tcpwrapped
9011/tcp open tcpwrapped
9040/tcp open tcpwrapped
9050/tcp open tcpwrapped
9071/tcp open tcpwrapped
9080/tcp open tcpwrapped
9081/tcp open tcpwrapped
9090/tcp open tcpwrapped
9091/tcp open tcpwrapped
9099/tcp open tcpwrapped
9100/tcp open jetdirect?
9101/tcp open jetdirect?
9102/tcp open jetdirect?
9103/tcp open jetdirect?
9110/tcp open tcpwrapped
9111/tcp open tcpwrapped
9200/tcp open tcpwrapped
9207/tcp open tcpwrapped
9220/tcp open tcpwrapped
9290/tcp open tcpwrapped
9415/tcp open tcpwrapped
9418/tcp open tcpwrapped
9485/tcp open tcpwrapped
9500/tcp open tcpwrapped
9502/tcp open tcpwrapped
9503/tcp open tcpwrapped
9535/tcp open tcpwrapped
9575/tcp open tcpwrapped
9593/tcp open tcpwrapped
9594/tcp open tcpwrapped
9595/tcp open tcpwrapped
9618/tcp open tcpwrapped
9666/tcp open tcpwrapped
9876/tcp open tcpwrapped
9877/tcp open tcpwrapped
9878/tcp open tcpwrapped
9898/tcp open tcpwrapped
9900/tcp open tcpwrapped
9917/tcp open tcpwrapped
9929/tcp open tcpwrapped

9943/tcp open tcpwrapped
9944/tcp open tcpwrapped
9968/tcp open tcpwrapped
9998/tcp open tcpwrapped
9999/tcp open tcpwrapped
10000/tcp open tcpwrapped
10001/tcp open tcpwrapped
10002/tcp open tcpwrapped
10003/tcp open tcpwrapped
10004/tcp open tcpwrapped
10009/tcp open tcpwrapped
10010/tcp open tcpwrapped
10012/tcp open tcpwrapped
10024/tcp open tcpwrapped
10025/tcp open tcpwrapped
10082/tcp open tcpwrapped
10180/tcp open tcpwrapped
10215/tcp open tcpwrapped
10243/tcp open tcpwrapped
10566/tcp open tcpwrapped
10616/tcp open tcpwrapped
10617/tcp open tcpwrapped
10621/tcp open tcpwrapped
10626/tcp open tcpwrapped
10628/tcp open tcpwrapped
10629/tcp open tcpwrapped
10778/tcp open tcpwrapped
11110/tcp open tcpwrapped
11111/tcp open tcpwrapped
11967/tcp open tcpwrapped
12000/tcp open tcpwrapped
12174/tcp open tcpwrapped
12265/tcp open tcpwrapped
12345/tcp open tcpwrapped
13456/tcp open tcpwrapped
13722/tcp open tcpwrapped
13782/tcp open tcpwrapped
13783/tcp open tcpwrapped
14000/tcp open tcpwrapped
14238/tcp open tcpwrapped
14441/tcp open tcpwrapped
14442/tcp open tcpwrapped
15000/tcp open tcpwrapped
15002/tcp open tcpwrapped

15003/tcp open tcpwrapped
15004/tcp open tcpwrapped
15660/tcp open tcpwrapped
15742/tcp open tcpwrapped
16000/tcp open tcpwrapped
16001/tcp open tcpwrapped
16012/tcp open tcpwrapped
16016/tcp open tcpwrapped
16018/tcp open tcpwrapped
16080/tcp open tcpwrapped
16113/tcp open tcpwrapped
16992/tcp open tcpwrapped
16993/tcp open tcpwrapped
17877/tcp open tcpwrapped
17988/tcp open tcpwrapped
18040/tcp open tcpwrapped
18101/tcp open tcpwrapped
18988/tcp open tcpwrapped
19101/tcp open tcpwrapped
19283/tcp open tcpwrapped
19315/tcp open tcpwrapped
19350/tcp open tcpwrapped
19780/tcp open tcpwrapped
19801/tcp open tcpwrapped
19842/tcp open tcpwrapped
20000/tcp open tcpwrapped
20005/tcp open tcpwrapped
20031/tcp open tcpwrapped
20221/tcp open tcpwrapped
20222/tcp open tcpwrapped
20828/tcp open tcpwrapped
21571/tcp open tcpwrapped
22939/tcp open tcpwrapped
23502/tcp open tcpwrapped
24444/tcp open tcpwrapped
24800/tcp open tcpwrapped
25734/tcp open tcpwrapped
25735/tcp open tcpwrapped
26214/tcp open tcpwrapped
27000/tcp open tcpwrapped
27352/tcp open tcpwrapped
27353/tcp open tcpwrapped
27355/tcp open tcpwrapped
27356/tcp open tcpwrapped

27715/tcp open tcpwrapped
28201/tcp open tcpwrapped
30000/tcp open tcpwrapped
30718/tcp open tcpwrapped
30951/tcp open tcpwrapped
31038/tcp open tcpwrapped
31337/tcp open tcpwrapped
32768/tcp open tcpwrapped
32769/tcp open tcpwrapped
32770/tcp open tcpwrapped
32771/tcp open tcpwrapped
32772/tcp open tcpwrapped
32773/tcp open tcpwrapped
32774/tcp open tcpwrapped
32775/tcp open tcpwrapped
32776/tcp open tcpwrapped
32777/tcp open tcpwrapped
32778/tcp open tcpwrapped
32779/tcp open tcpwrapped
32780/tcp open tcpwrapped
32781/tcp open tcpwrapped
32782/tcp open tcpwrapped
32783/tcp open tcpwrapped
32784/tcp open tcpwrapped
32785/tcp open tcpwrapped
33354/tcp open tcpwrapped
33899/tcp open tcpwrapped
34571/tcp open tcpwrapped
34572/tcp open tcpwrapped
34573/tcp open tcpwrapped
35500/tcp open tcpwrapped
38292/tcp open tcpwrapped
40193/tcp open tcpwrapped
40911/tcp open tcpwrapped
41511/tcp open tcpwrapped
42510/tcp open tcpwrapped
44176/tcp open tcpwrapped
44442/tcp open tcpwrapped
44443/tcp open tcpwrapped
44501/tcp open tcpwrapped
45100/tcp open tcpwrapped
48080/tcp open tcpwrapped
49152/tcp open tcpwrapped
49153/tcp open tcpwrapped

49154/tcp open tcpwrapped
49155/tcp open tcpwrapped
49156/tcp open tcpwrapped
49157/tcp open tcpwrapped
49158/tcp open tcpwrapped
49159/tcp open tcpwrapped
49160/tcp open tcpwrapped
49161/tcp open tcpwrapped
49163/tcp open tcpwrapped
49165/tcp open tcpwrapped
49167/tcp open tcpwrapped
49175/tcp open tcpwrapped
49176/tcp open tcpwrapped
49400/tcp open tcpwrapped
49999/tcp open tcpwrapped
50000/tcp open tcpwrapped
50001/tcp open tcpwrapped
50002/tcp open tcpwrapped
50003/tcp open tcpwrapped
50006/tcp open tcpwrapped
50300/tcp open tcpwrapped
50389/tcp open tcpwrapped
50500/tcp open tcpwrapped
50636/tcp open tcpwrapped
50800/tcp open tcpwrapped
51103/tcp open tcpwrapped
51493/tcp open tcpwrapped
52673/tcp open tcpwrapped
52822/tcp open tcpwrapped
52848/tcp open tcpwrapped
52869/tcp open tcpwrapped
54045/tcp open tcpwrapped
54328/tcp open tcpwrapped
55055/tcp open tcpwrapped
55056/tcp open tcpwrapped
55555/tcp open tcpwrapped
55600/tcp open tcpwrapped
56737/tcp open tcpwrapped
56738/tcp open tcpwrapped
57294/tcp open tcpwrapped
57797/tcp open tcpwrapped
58080/tcp open tcpwrapped
60020/tcp open tcpwrapped
60443/tcp open tcpwrapped

61532/tcp open tcpwrapped
61900/tcp open tcpwrapped
62078/tcp open tcpwrapped
63331/tcp open tcpwrapped
64623/tcp open tcpwrapped
64680/tcp open tcpwrapped
65000/tcp open tcpwrapped
65129/tcp open tcpwrapped
65389/tcp open tcpwrapped

Nmap scan report for 186.146.1.85.dynamic.wline.res.cust.swisscom.ch (85.1.146.186)
Host is up (0.11s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
25/tcp filtered smtp
53/tcp filtered domain
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
1145/tcp filtered x9-icue
9200/tcp filtered wap-wsp
45100/tcp filtered unknown

Nmap scan report for pl95929.ag1001.nttpc.ne.jp (1.33.102.185)
Host is up (0.19s latency).
All 1000 scanned ports on pl95929.ag1001.nttpc.ne.jp (1.33.102.185) are in ignored states.
Not shown: 850 filtered tcp ports (no-response), 150 closed tcp ports (conn-refused)

Nmap scan report for 36.80.174.222
Host is up.
All 1000 scanned ports on 36.80.174.222 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 116.124.83.121
Host is up (0.19s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
113/tcp closed ident

Nmap scan report for 178-116-144-99.access.telenet.be (178.116.144.99)
Host is up (0.13s latency).

Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
8080/tcp closed http-proxy

Nmap scan report for PATTERSON-U.ear2.Denver1.Level3.net (4.14.112.222)
Host is up.
All 1000 scanned ports on PATTERSON-U.ear2.Denver1.Level3.net (4.14.112.222) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 123.135.15.161
Host is up.
All 1000 scanned ports on 123.135.15.161 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 117.206.65.36
Host is up (0.27s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
513/tcp closed login
514/tcp closed shell
593/tcp closed http-rpc-epmap
5555/tcp closed freeciv
8600/tcp closed asterix

Nmap scan report for 047-033-188-038.res.spectrum.com (47.33.188.38)
Host is up (0.091s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
5101/tcp open admdog?

Nmap scan report for 118.33.172.166
Host is up (0.22s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
25/tcp filtered smtp
80/tcp filtered http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
179/tcp filtered bgp
445/tcp filtered microsoft-ds
2869/tcp filtered icslap
4444/tcp filtered krb524
4662/tcp filtered edonkey

8899/tcp filtered ospf-lite
9000/tcp filtered cslistener
52869/tcp filtered unknown

Nmap scan report for a104-119-72-137.deploy.static.akamaitechnologies.com (104.119.72.137)
Host is up (0.080s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open http   AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-title: Invalid URL
443/tcp open ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| ssl-cert: Subject: commonName=api.vmh.univision.com/organizationName=Univision Communications Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:api.vmh.univision.com, DNS:www.tudn.tv, DNS:www.tudn.com, DNS:wsc.tudn.com
| Not valid before: 2022-11-15T00:00:00
|_Not valid after: 2023-11-15T23:59:59
| tls-nextprotoneg:
| http/1.1
|_ http/1.0
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
| http/1.1
|_ http/1.0
|_http-title: Invalid URL

Nmap scan report for softbank060127252001.bbtec.net (60.127.252.1)
Host is up (0.19s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT   STATE   SERVICE   VERSION
25/tcp   filtered smtp
80/tcp   filtered http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
340/tcp   filtered unknown
445/tcp   filtered microsoft-ds
2103/tcp filtered zephyr-clt
8000/tcp filtered http-alt
55555/tcp filtered unknown
55600/tcp filtered unknown

Nmap scan report for client-104-168-160-196.hostwindsdns.com

(104.168.160.196)
Host is up (0.064s latency).
Not shown: 931 filtered tcp ports (no-response), 58 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
| ssl-cert: Subject: commonName=sea-shared-23.hostwindsdns.com
| Subject Alternative Name: DNS:sea-shared-23.hostwindsdns.com
| Not valid before: 2023-10-06T00:00:00
|_Not valid after: 2024-01-04T23:59:59
|_ssl-date: TLS randomness does not represent time
53/tcp open domain PowerDNS Authoritative Server 4.7.3
| dns-nsid:
| NSID: sea-shared-23.hostwindsdns.com (7365612d7368617265642d32332e686f737477696e6473646e732e636f6d)
| id.server: sea-shared-23.hostwindsdns.com
|_ bind.version: PowerDNS Authoritative Server 4.7.3 (built Apr 25 2023 12:34:07 by root@bh-centos-7.dev.cpanel.net)
80/tcp open http Apache httpd
|_http-server-header: Apache
|_http-title: 508 Resource Limit Is Reached
110/tcp open pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=*.hostwindsdns.com
| Subject Alternative Name: DNS:*.hostwindsdns.com, DNS:hostwindsdns.com
| Not valid before: 2023-02-06T00:00:00
|_Not valid after: 2024-03-05T23:59:59
|_pop3-capabilities: USER SASL(PLAIN LOGIN) AUTH-RESP-CODE STLS TOP PIPELINING UIDL CAPA RESP-CODES
143/tcp open imap Dovecot imapd
|_imap-capabilities: IDLE OK ENABLE post-login Pre-login have STARTTLS AUTH=PLAIN more ID LOGIN-REFERRALS capabilities LITERAL+ listed AUTH=LOGINA0001 NAMESPACE SASL-IR IMAP4rev1
| ssl-cert: Subject: commonName=*.hostwindsdns.com
| Subject Alternative Name: DNS:*.hostwindsdns.com, DNS:hostwindsdns.com
| Not valid before: 2023-02-06T00:00:00
|_Not valid after: 2024-03-05T23:59:59
443/tcp open ssl/http Apache httpd
| ssl-cert: Subject: commonName=daedalia.net
| Subject Alternative Name: DNS:daedalia.net, DNS:cpanel.daedalia.net, DNS:cpcalendars.daedalia.net, DNS:cpcontacts.daedalia.net, DNS:mail.daedalia.net, DNS:webdisk.daedalia.net, DNS:webmail.daedalia.net, DNS:www.daedalia.net
| Not valid before: 2023-09-17T00:00:00
|_Not valid after: 2023-12-16T23:59:59

|_http-server-header: Apache
|_http-title: 508 Resource Limit Is Reached
465/tcp open ssl/smtp Exim smtpd 4.96.2
| ssl-cert: Subject: commonName=*.hostwindsdns.com
| Subject Alternative Name: DNS:*.hostwindsdns.com, DNS:hostwindsdns.com
| Not valid before: 2023-02-06T00:00:00
|_Not valid after: 2024-03-05T23:59:59
| smtp-commands: sea-shared-23.hostwindsdns.com Hello bras-base-stcton1063w-grc-09-76-71-97-173.dsl.bell.ca [76.71.97.173], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
587/tcp open smtp   Exim smtpd 4.96.2
| ssl-cert: Subject: commonName=*.hostwindsdns.com
| Subject Alternative Name: DNS:*.hostwindsdns.com, DNS:hostwindsdns.com
| Not valid before: 2023-02-06T00:00:00
|_Not valid after: 2024-03-05T23:59:59
| smtp-commands: sea-shared-23.hostwindsdns.com Hello bras-base-stcton1063w-grc-09-76-71-97-173.dsl.bell.ca [76.71.97.173], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
993/tcp open imaps?
| ssl-cert: Subject: commonName=*.hostwindsdns.com
| Subject Alternative Name: DNS:*.hostwindsdns.com, DNS:hostwindsdns.com
| Not valid before: 2023-02-06T00:00:00
|_Not valid after: 2024-03-05T23:59:59
|_imap-capabilities: IDLE OK ENABLE post-login Pre-login have capabilities AUTH=PLAIN more LOGIN-REFERRALS ID NAMESPACE listed AUTH=LOGINA0001 LITERAL+ SASL-IR IMAP4rev1
995/tcp open pop3s?
| ssl-cert: Subject: commonName=*.hostwindsdns.com
| Subject Alternative Name: DNS:*.hostwindsdns.com, DNS:hostwindsdns.com
| Not valid before: 2023-02-06T00:00:00
|_Not valid after: 2024-03-05T23:59:59
|_pop3-capabilities: CAPA AUTH-RESP-CODE USER SASL(PLAIN LOGIN) PIPELINING UIDL RESP-CODES TOP
3306/tcp open mysql   MySQL 5.5.5-10.0.38-MariaDB-cll-lve
| mysql-info:
| Protocol: 10
| Version: 5.5.5-10.0.38-MariaDB-cll-lve
| Thread ID: 24333587
| Capabilities flags: 63487
| Some Capabilities: ODBCClient, LongColumnFlag, Support41Auth,

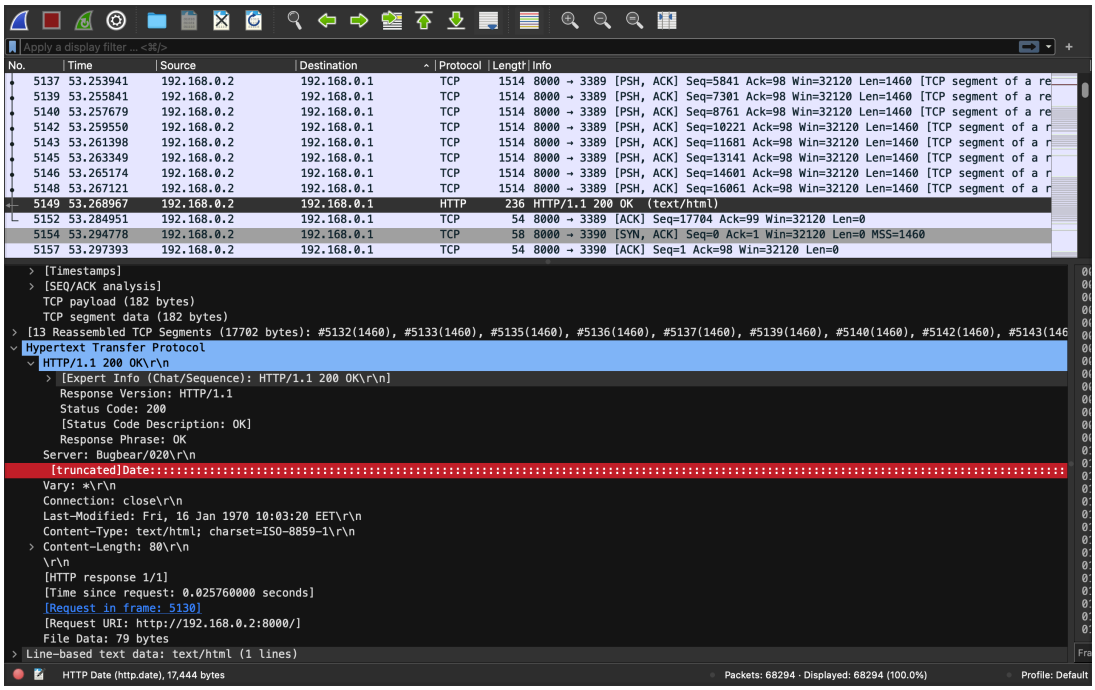
ConnectWithDatabase, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, SupportsCompression, LongPassword, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, InteractiveClient, FoundRows, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: aiiSC5}:H9'UX9Sx!86D
|_ Auth Plugin Name: mysql_native_password
Service Info: Host: sea-shared-23.hostwindsdns.com

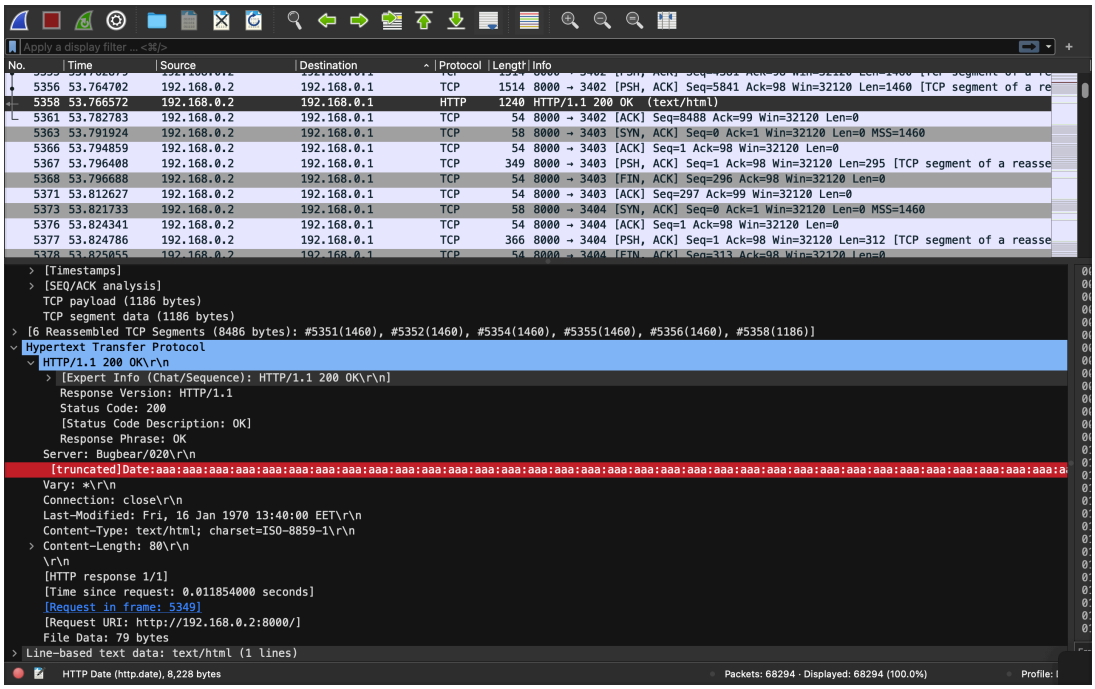
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 17 IP addresses (17 hosts up) scanned in 1902.98 seconds
gurashishanand@gee ~ %

3(Log Analysis):-

c05-http-reply-r1.pcap

I found a very unusual pattern in the date field of some network packets. The date field of some network packets has a very unusual formatting which appears to be irregular and contains unusual value which could be a potential data corruption or an attempt to exploit a loophole. This could currently be far from being a buffer overflow attack, but could be an attempt to provoke buffer overflow or some other vulnerability. Another reason why I think this to be malicious is because of the fact that the whole packet interchange is going on between port 8000(which is not one of the well known ports) and port 3389(RDP). Also, the biggest reason I think that this is unusual activity is for that fact that there are multiple connection attempts from the same source IP and to the same destination IP(with different false values), which seems like a deliberate attempt to manipulate data transmission.





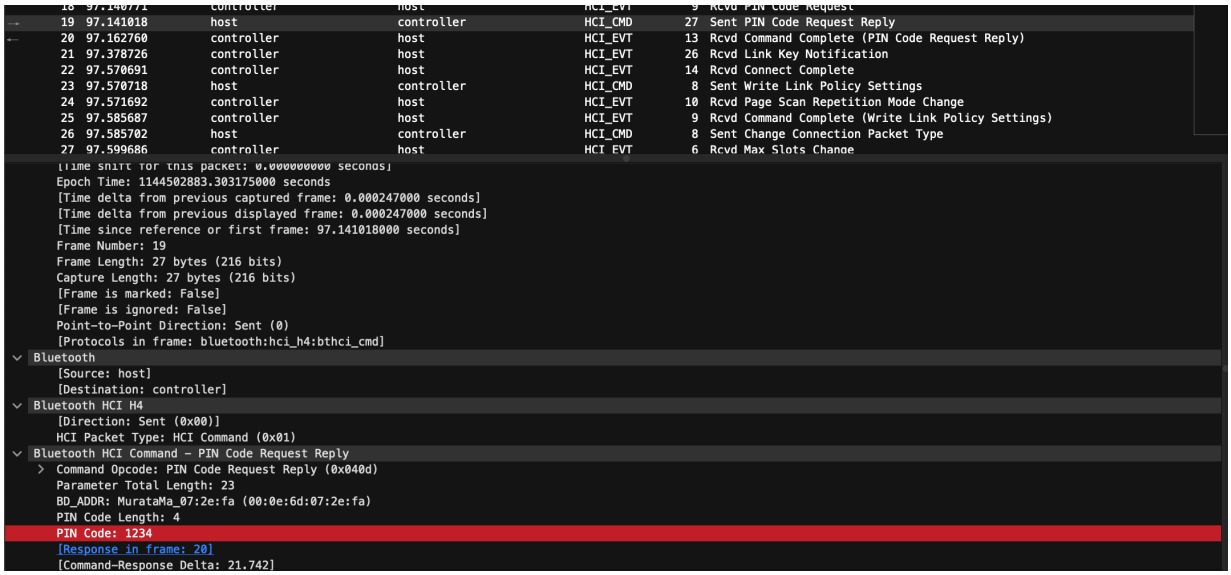
Smb-browser-collections.pcap

This file has a high number of browser election requests, name queries responses, and registration responses. The activity captured by Wireshark might not necessarily be malicious, but it is worth investigating due to the unusual number of requests and responses, and that too on the same destination. If this doesn't turn out to legitimate, this could be a ARP poisoning attack.

13	241.738484	192.168.123.1	192.168.123.255	BROWSER	233	Browser Election Request
14	241.848104	192.168.123.2	192.168.123.255	BROWSER	235	Browser Election Request
15	242.738524	192.168.123.1	192.168.123.255	BROWSER	233	Browser Election Request
16	242.754362	192.168.123.2	192.168.123.255	BROWSER	235	Browser Election Request
17	243.738568	192.168.123.1	192.168.123.255	BROWSER	233	Browser Election Request
18	243.832540	192.168.123.2	192.168.123.255	BROWSER	235	Browser Election Request
19	244.738618	192.168.123.1	192.168.123.255	BROWSER	233	Browser Election Request
20	244.770010	192.168.123.2	192.168.123.255	BROWSER	235	Browser Election Request

Bluetooth1.cap

There are multiple bluetooth requests and responses captured in this file. One frame in fact exposes a bluetooth pin in plain text, which is 1234. This might not be a big deal, but an attacker can potentially use the exposed pin for bluejacking or bluesnarfing, perhaps both.



Bfd-raw-auth

This file consists of a password exposed in plain text in its UDP logs.

```
User Datagram Protocol, Src Port: 1024, Dst Port: 3784
    Source Port: 1024
    Destination Port: 3784
    Length: 41
    Checksum: 0x7231 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (33 bytes)
BFD Control message
    001. .... = Protocol Version: 1
    ...0 0000 = Diagnostic Code: No Diagnostic (0x00)
    01.. .... = Session State: Down (0x1)
  > Message Flags: 0x44, Authentication Present: Set
    Detect Time Multiplier: 5 (= 5000 ms Detection time)
    Message Length: 33 bytes
    My Discriminator: 0x00000001
    Your Discriminator: 0x00000000
    Desired Min TX Interval: 1000 ms (1000000 us)
    Required Min RX Interval: 1000 ms (1000000 us)
    Required Min Echo Interval:    0 ms (0 us)
  Authentication: Simple Password
        Authentication Type: Simple Password (1)
        Authentication Length: 9 bytes
        Authentication Key ID: 2
        Password: secret
```

smtp.pcap

The network traffic captured in this file exposes login credentials of a user. On frame 12, it displays that hash of the username that was trying to connect to 74.53.140.153 using the SMTP protocol. The hash was easily decrypted on 'hashes.com'. Similarly, on frame 14, I got the base64 hash of the password which I could easily decrypt on my terminal. The credentials I got were gurpartap@patriots.in:punjab@123.

12	1.419595	10.10.1.4	74.53.140.153	SMTP	84	C: User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72	S: 334 UGFzc3dvcmQ6
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72	C: Pass: cHVuamFiQDEyMw==

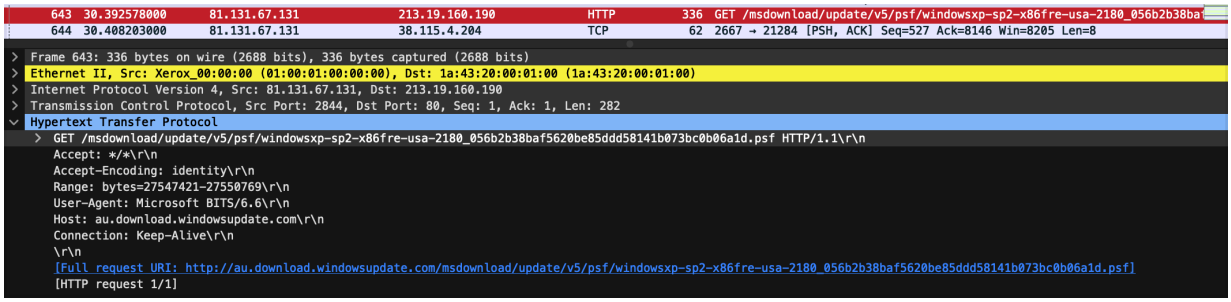
✔ **Found:**

```
Z3VycGFydGFwQHBhdHJpb3RzLmlu:gurpartap@patriots.in
```

```
gurashishanand@gee ~ % echo cHVuamFiQDEyMw== | base64 -d
punjab@123%
gurashishanand@gee ~ %
```

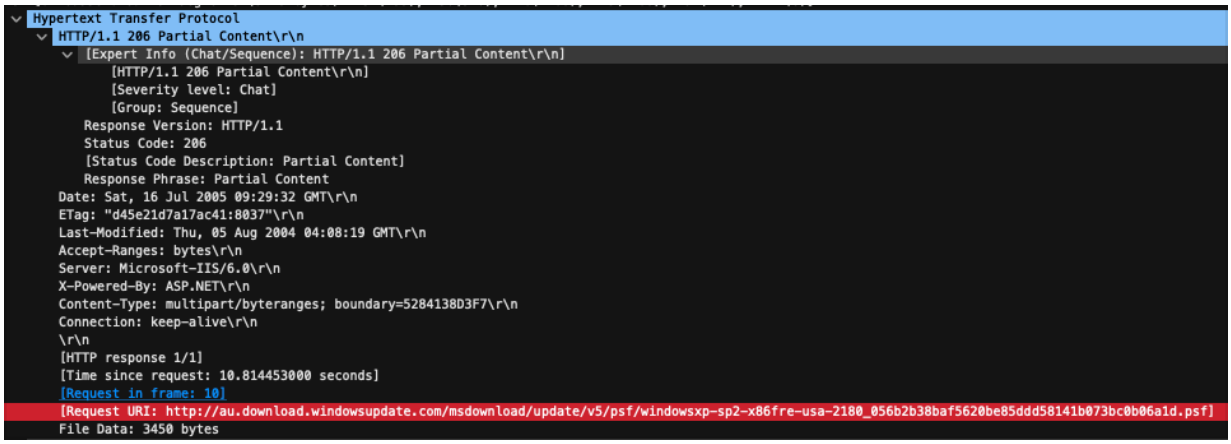
FTPv6-2.pcap

In this file, on frame 643, I noticed an update. The problem is that the update is for windowsXP which is outdated and extremely vulnerable when it comes to RCE exploits.



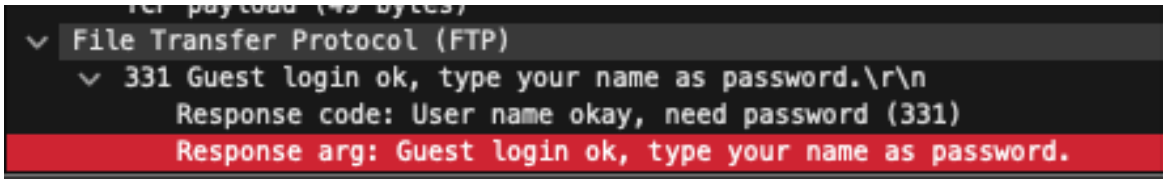
FTPv6-1.pcap

On frame 221, I found a similar vulnerability to what I found in FTPv6-2.pcap, which is a machine requesting an update thats running Windows XP, which is outdated and extremely vulnerable to RCE exploits.

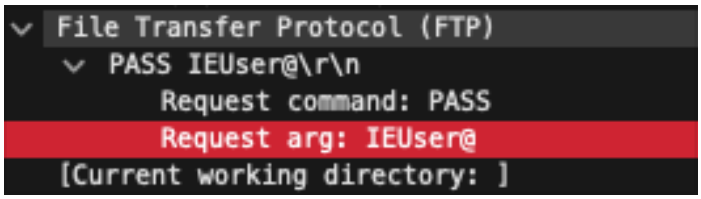


On frame 267 and 268, we kind of notice a FTP login leak where the FTP server asks the user to enter their username as the password, and we see the input in plain text as IEUser@. This information can potentially be used to access the FTP server of the organization.

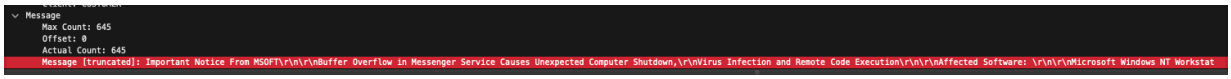
Frame 267:-



Frame 268:-

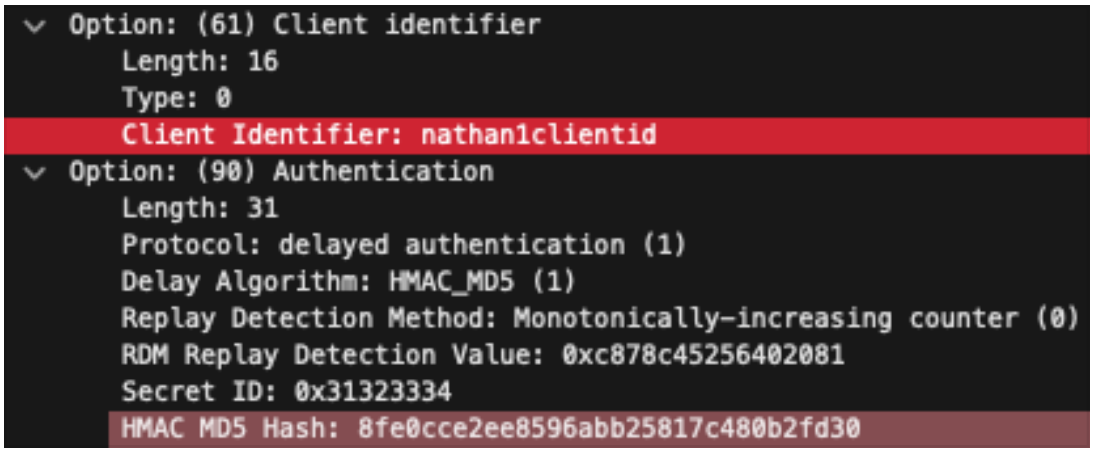


On frame 301, we detect a computer shutdown because of a virus caused by buffer overflow which is carried out by remote code execution.



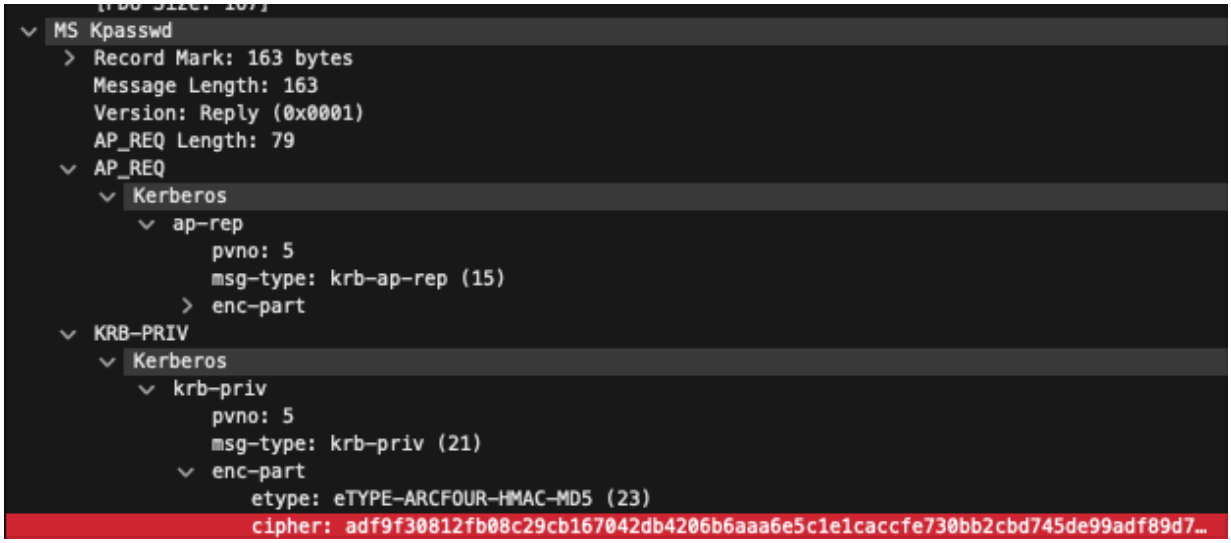
dhcp-auth.pcap

The only frame available on this file exposed the login credentials to the DHCP server. The username is displayed in plain text, and the password is encrypted with a MD5 hash, which is very easy to decrypt.



KPASSWD_tcp.cap

What I found on frame 15 could be the hexadecimal password of kerberos. Even though this encryption is strong, it could potentially be cracked using offline brute forcing, rainbow table attacks, etc.



4.(Vulnerability Prioritization)

Critical Priority:-

- **FTPv6-2.pcap(Wireshark):** The update for Windows XP introduces a potential vulnerability to RCE exploits. Exploiting this vulnerability could lead to a compromised system, which may also be used to pivot to other systems.

- **FTPv6-1.pcap(Wireshark):** Similar to FTPv6-2.pcap, it exposes a Windows XP system to RCE exploits and includes an FTP login leak, potentially allowing unauthorized access through FTP and a pivot risk through RCE exploits on the windows xp system.

- **smtp.pcap(Wireshark):** Exposing login credentials for an SMTP server poses a serious threat, as it could lead to unauthorized access or misuse of email accounts.

- **Bfd-raw-auth(Wireshark):** Exposing passwords in plain text in UDP logs is a critical security issue, as it could lead to unauthorized access or misuse.

High Priority:-

- **KPASSWD_tcp.cap(Wireshark):** The exposure of a hexadecimal password for Kerberos, although strongly encrypted, poses a risk if attackers attempt offline brute forcing or rainbow table attacks.

- **c05-http-reply-r1.pcap(Wireshark):** Unusual patterns in the date field, multiple connection attempts, and manipulation of data transmission suggest potential malicious activity. Investigation is warranted to understand the nature and intent of this activity.

- **Bluetooth1.cap(Wireshark):** Exposing a Bluetooth PIN in plain text poses a risk for bluejacking or bluesnarfing attacks. It should be addressed to prevent potential Bluetooth-related security issues.

Medium Priority:-

- **dhcp-auth.pca(Wireshark):** Exposing login credentials to the DHCP server, even with MD5 encryption, requires attention to prevent potential unauthorized access. Plus, its really important to use better hashing algorithms and MD5 is not hard to crack.

Low Priority:

- **Smb-browser-collections.pcap(Wireshark):** The high number of browser election requests may indicate ARP poisoning. Further investigation is needed to determine the legitimacy of this activity.

- **47.33.188.38(Nmap):** The unidentified service on port 5101/tcp raises concerns. Further investigation is needed to understand the nature of the service and address potential vulnerabilities.

- **104.168.160.196(Nmap):** The host exposes multiple services with potential vulnerabilities, including FTP, DNS, HTTP, and email. Regular updates and configuration checks are necessary to mitigate these risks.

- **13.34.43.135.24(Nmap):** The high number of open ports with unidentified services raises concerns. Further investigation is needed to identify potential vulnerabilities and services running on these ports.

Additional Notes:

- Regularly updating and patching Windows XP systems (FTPv6-1.pcap, FTPv6-2.pcap) is crucial to mitigate known vulnerabilities.
- Implementing security measures for Bluetooth devices (Bluetooth1.cap) is essential to prevent unauthorized access.
- Monitoring and securing SMTP servers (smtp.pcap) should be a priority

to protect sensitive email communication.
- The unusual network activity in c05-http-reply-r1.pcap (Vulnerability 1) and the high number of browser election requests in Smb-browser-collections.pcap (Vulnerability 2) may require further analysis to determine the nature of the activity and potential threats.

What I learned:-

As a person who’s had more time with red teaming than blue teaming, this was great fun. It was nice to learn about various public resources of information and of course, the OSINT framework. It was nice to learn how to filter out hosts by finding out which ones are up using a bash script to ping all at once, thereby finding out which ones are responding to pings. The sprint definitely helped me to develop skills on Wireshark, to search for multiple ports and services, following TCP and UDP streams, and trying to read between the lines. Overall, this sprint really helped me to develop skills in vulnerability assessment and I surely feel more confident in doing something similar in the future.