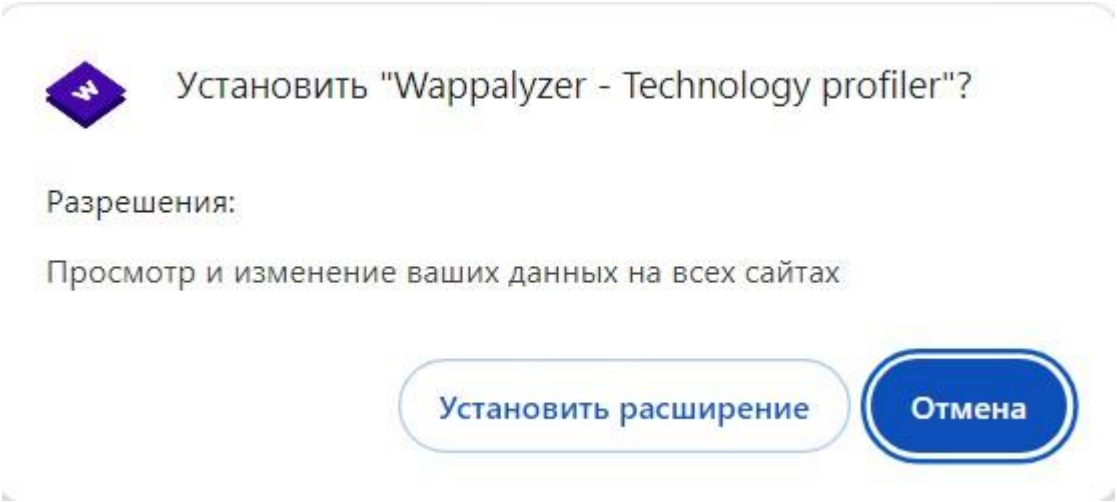
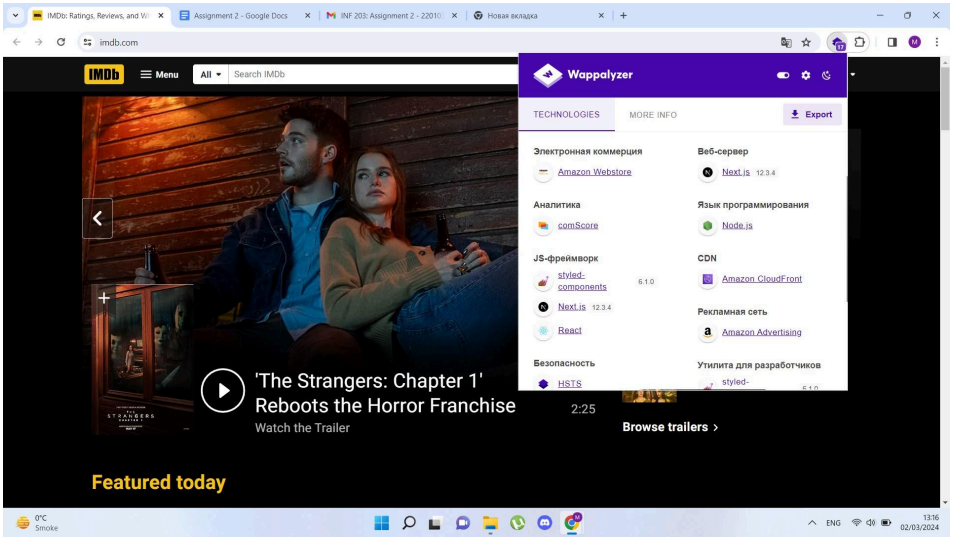
Berikov Miras
220103187

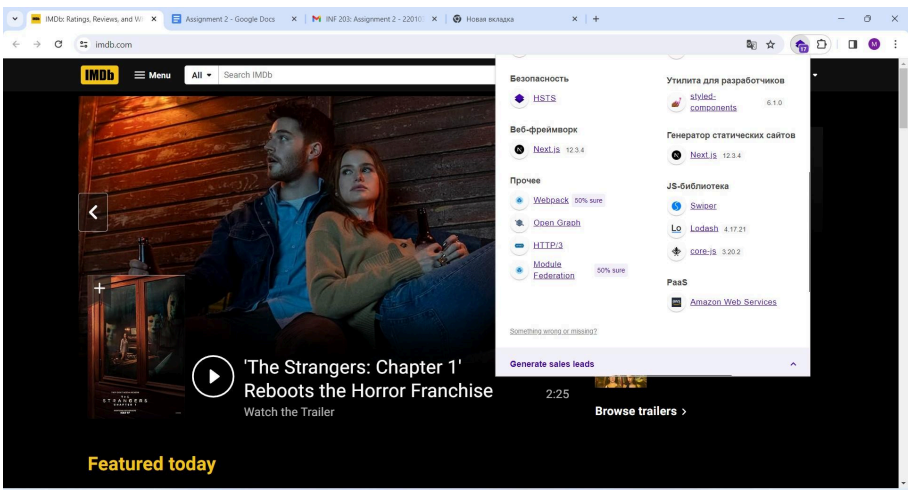
1) Investigate and identify the tools the website uses for analytics and tracking.



Wappalyzer detects the technologies used by websites, so we install it on our browser

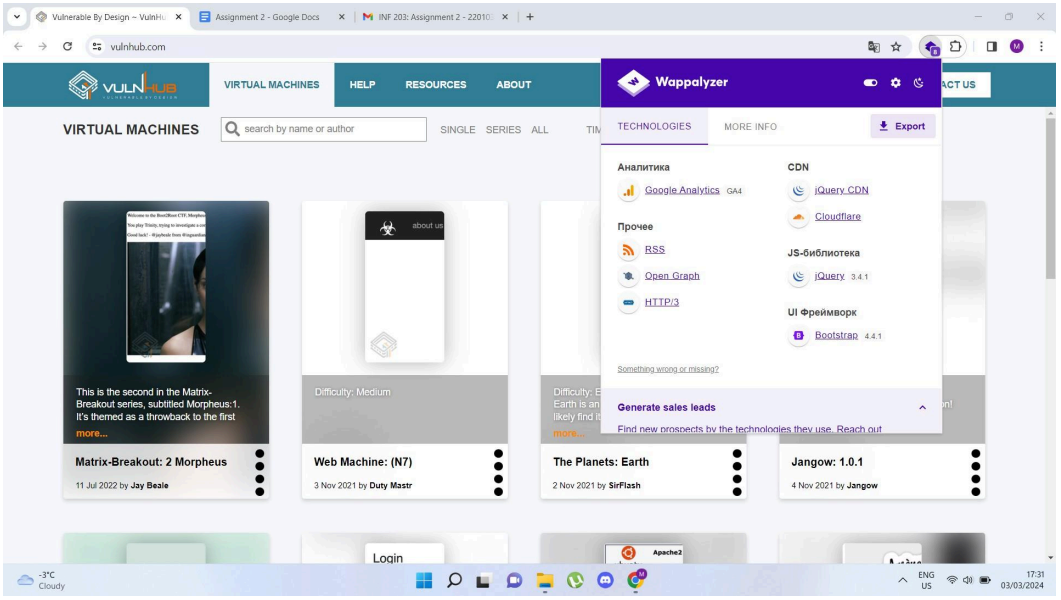
1 - imdb.com





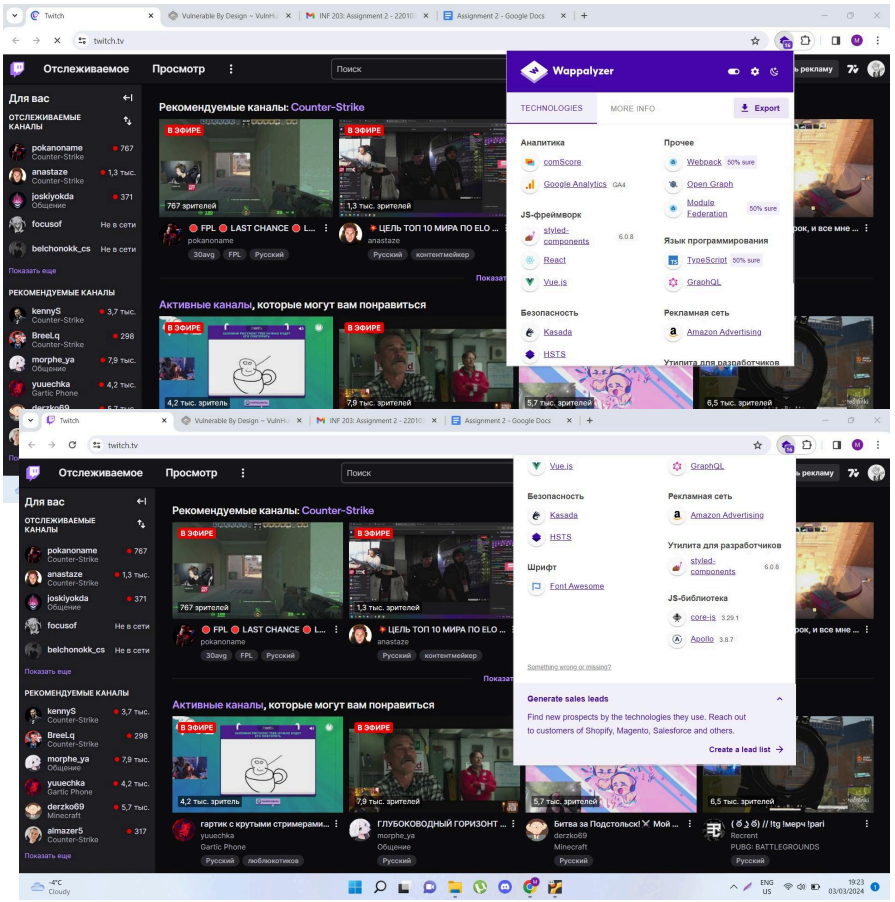
1. **Amazon Webstore** - developed by Amazon, a tool that can track user purchases on IMDb.
2. **comScore** - provides website analytics, including tracking visitor demographics, interests, and behavior on IMDb.
3. **Amazon Advertising** - tracks the performance of ads on IMDb.

2 - vulnhub.com



Google Analytics - the most popular website analytics platform.

3 - twitch.tv



1. **comScore** - provides website analytics, including tracking visitor demographics, interests, and behavior on Twitch.
2. **Google Analytics** - the most popular website analytics platform.
3. **Amazon Advertising** - tracks the performance of ads on Twitch.

2) Identify the technology stack that is used on the website.

Again we are using Wappalyzer so that we can identify the technology stack (All screens are on the first question)

1 - imdb.com

JS-framework: Next.js, React, styled-components; **Programming Language:** Node.js; **Security:** HSTS, **JS Library:** Swiper, Lodash, core-js

2 - vulnhub.com

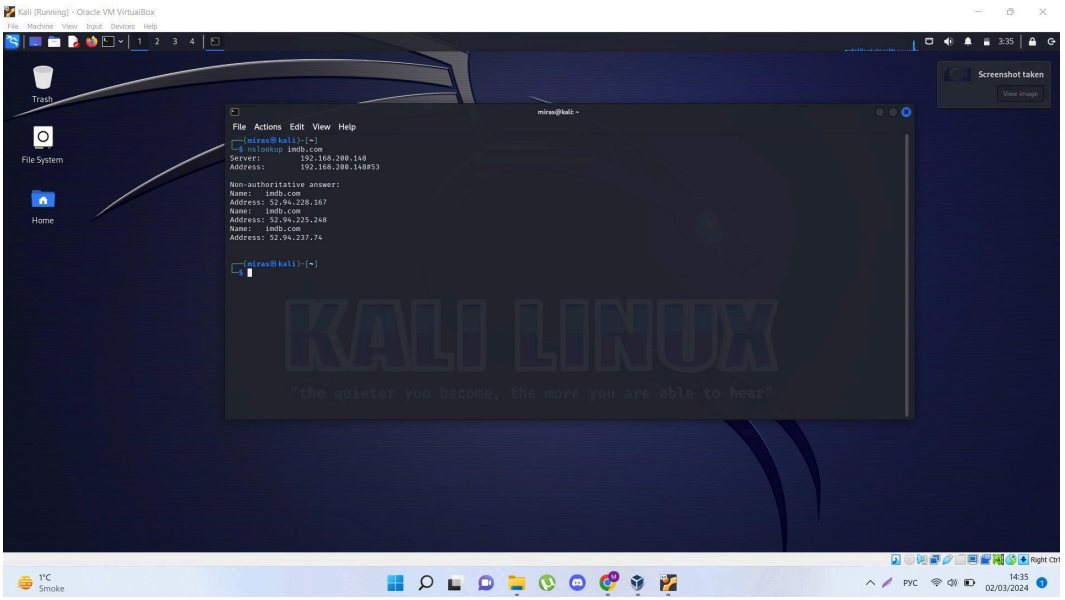
UI Framework: Bootstrap; **JS-library**: jQuery; **CDN:** jQuery CDN, Cloudflare

3 - twitch.tv

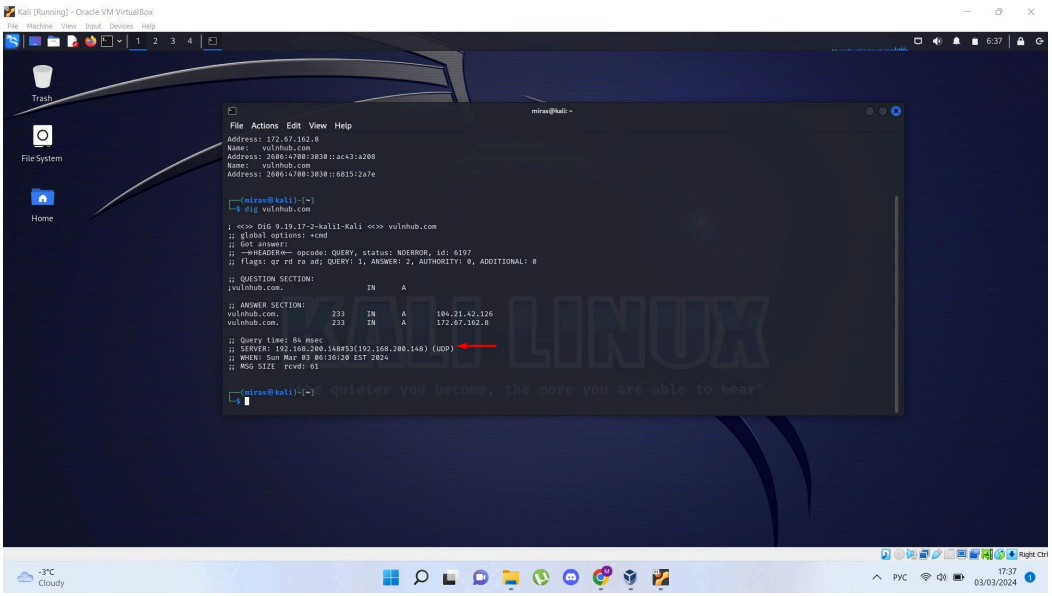
JS-framework: styled-components, React, Vue.js; **Programming Language:** TypeScript, GraphQL; **Security:** Kasada**,** HSTS, **JS Library:** core-js, Apollo

3) Find the IP address or addresses associated with the domain.

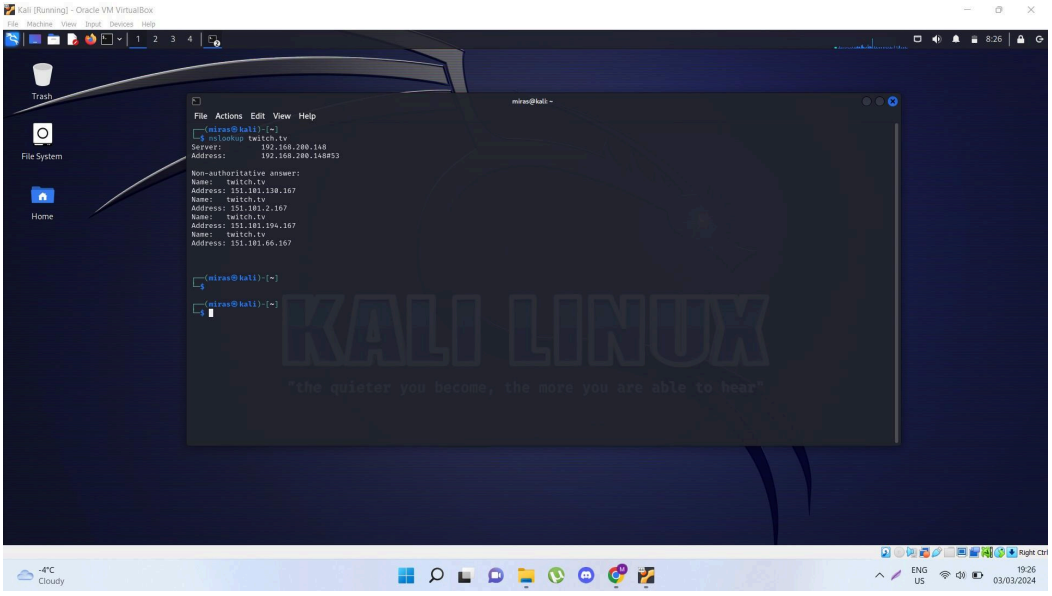
1 - imdb.com



2 - vulnhub.com



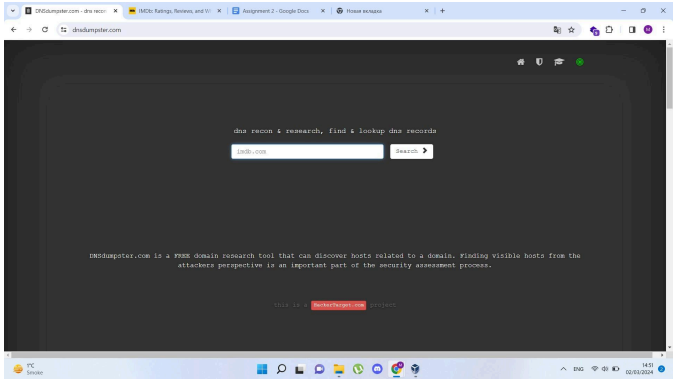
3 - twitch.tv

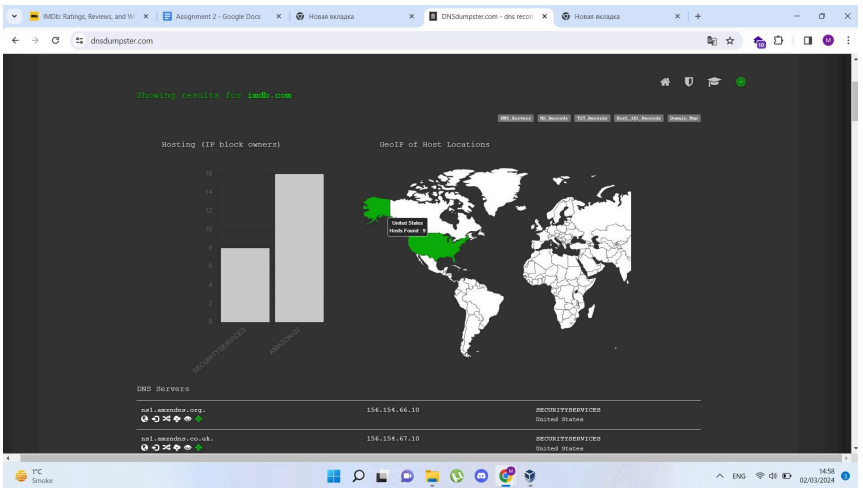


4) Conduct a subdomain enumeration to identify all subdomains associated with the target domain.

Dnsdumpster.com - a free website that allows you to find information about DNS records for a given domain.

1 - imdb.com

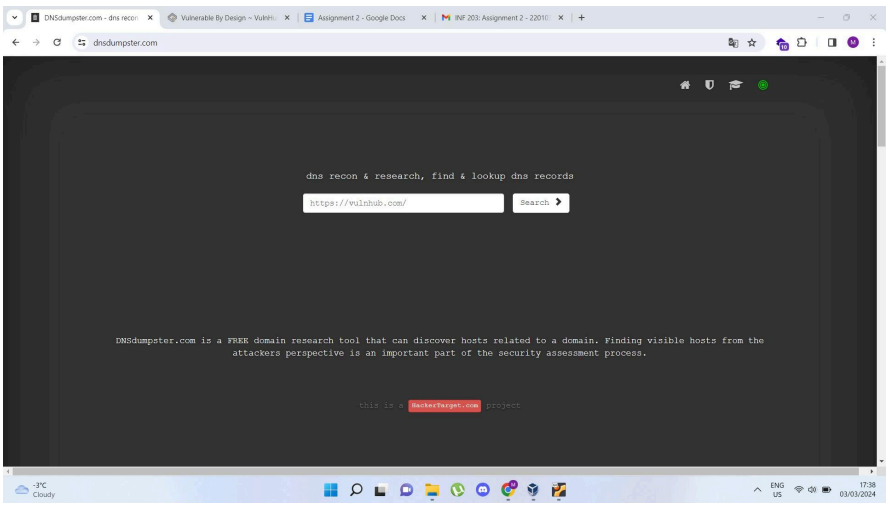


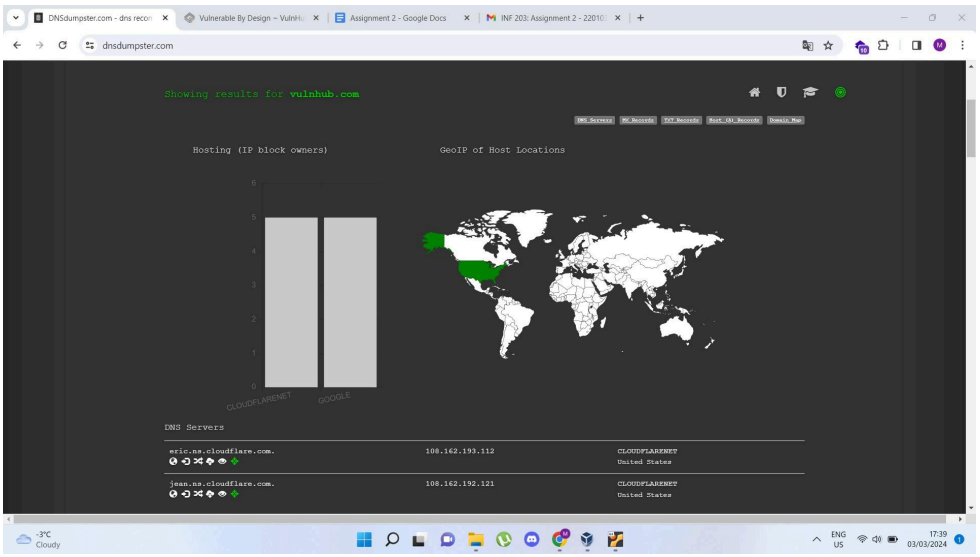


Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

origin-www-uw2.imdb.com HTTP: Server	52.119.171.76	AMAZON-02 United States
app.dd.imdb.com	52.94.225.250	AMAZON-02 United States
us.dd.imdb.com HTTP: Server	52.94.228.167	AMAZON-02 United States
webservice.imdb.com HTTP: Server	52.94.228.186	AMAZON-02 United States
secure.imdb.com HTTP: Server	52.94.237.74	AMAZON-02 United States
contribute.imdb.com HTTP: Server	52.94.228.191	AMAZON-02 United States
graphql.imdb.com	108.138.106.47 server-108-138-106-47.jfk50.r.cloudfront.net	AMAZON-02 United States
dev.graphql.imdb.com	108.138.246.59 server-108-138-246-59.sfo5.r.cloudfront.net	AMAZON-02 United States
opf-m.imdb.com	52.94.225.254	AMAZON-02 United States
origin-m.imdb.com	52.94.225.254	AMAZON-02 United States
origin-pro.imdb.com HTTP: Server	52.94.228.166	AMAZON-02 United States
origin-help.imdb.com HTTP: Server	52.94.235.171	AMAZON-02 United States
developer.imdb.com	18.160.10.9 server-18-160-10-9.iad12.r.cloudfront.net	AMAZON-02 United States
origin-www.imdb.com HTTP: Server	52.94.225.248	AMAZON-02 United States
apx-security.imdb.com HTTP: Server	52.46.149.74	AMAZON-02 United States

2 - vulnhub.com

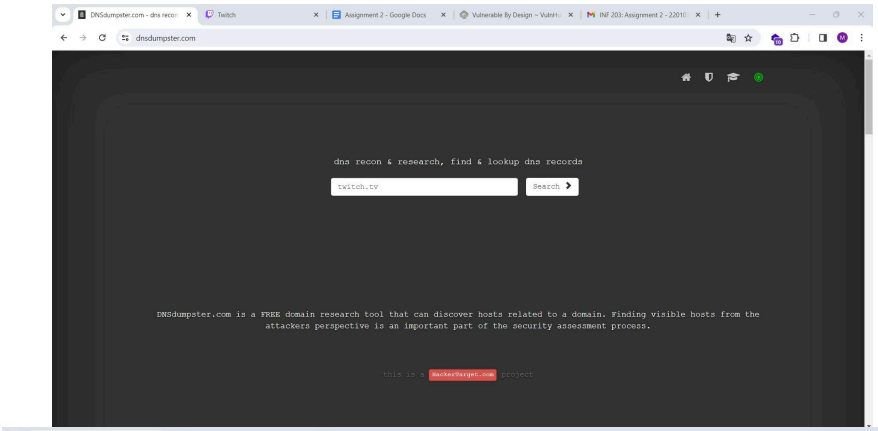


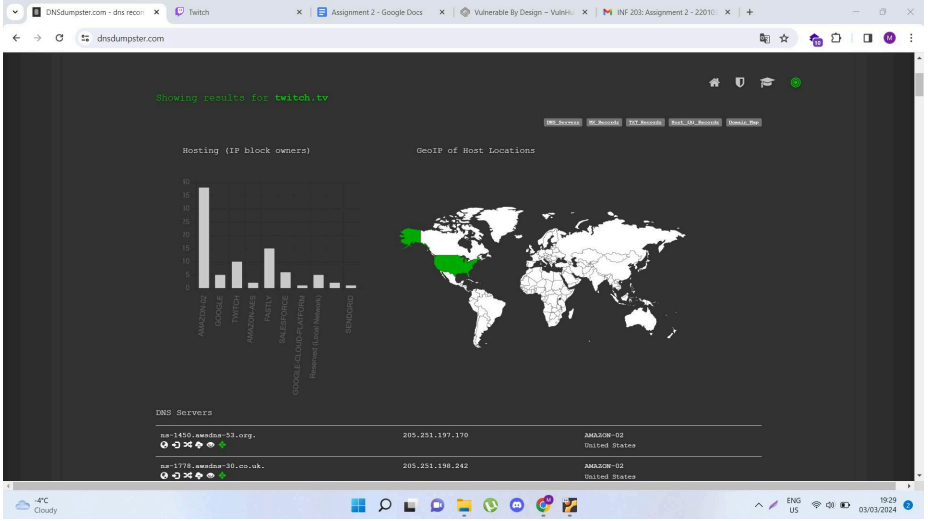


Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

download.vulnhub.com HTTP: cloudflare	172.67.162.8	CLOUDFLARENET United States
staging.vulnhub.com HTTP: cloudflare	172.67.162.8	CLOUDFLARENET United States
www.vulnhub.com HTTP: cloudflare	104.21.42.126	CLOUDFLARENET unknown

3 - twitch.tv



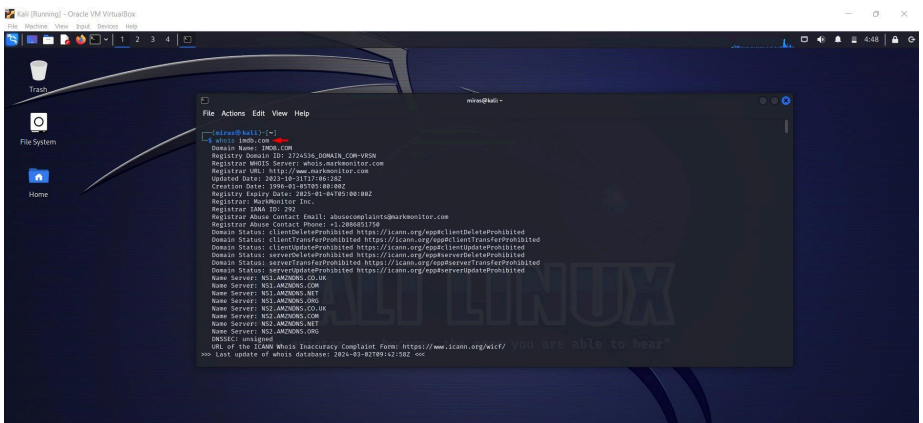


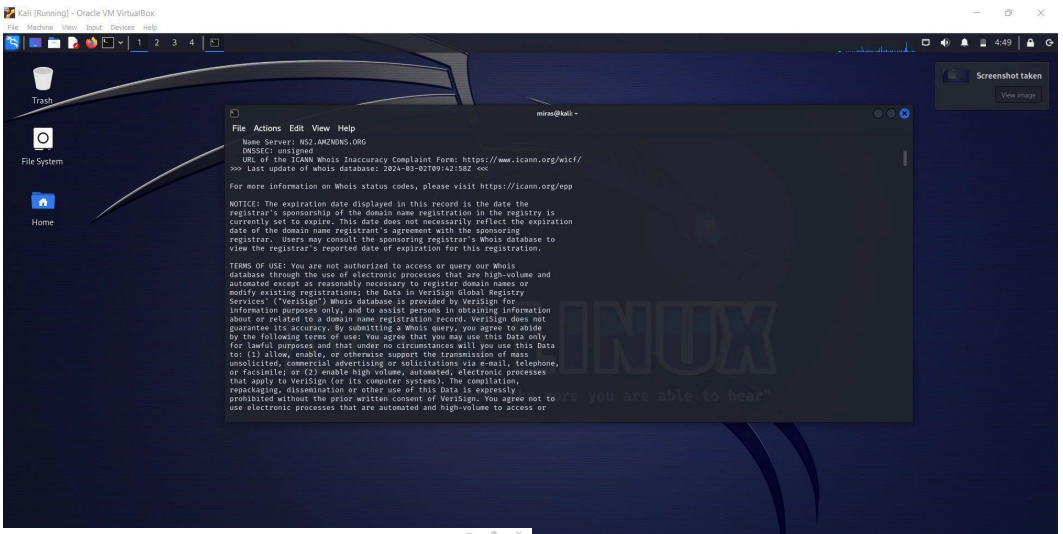
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

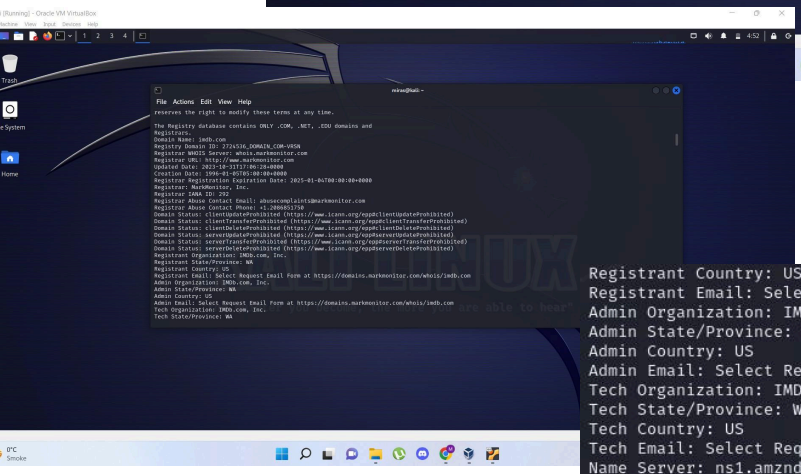
live2.twitch.tv	199.9.251.241	TWITCH United States
mail4.twitch.tv	199.9.253.87	TWITCH United States
mail6.twitch.tv	199.9.248.71	TWITCH United States
ntp-6ec8dc.twitch.tv	199.9.249.212	TWITCH United States
vmetric.twitch.tv HTTP: Apache	34.228.35.140	AMAZON-AES ec2-34-228-35-140.compute-1.amazonaws.com United States
rc.twitch.tv HTTP: Varnish HTTP TECH: varnish	151.101.194.167	FASTLY United States
id.twitch.tv HTTP: nginx/1.4.6 (Ubuntu) HTTP TECH: Ubuntu nginx,1.4.6 Ubuntu nginx,1.4.6 Angular	35.155.236.18	AMAZON-02 ec2-35-155-236-18.us-west-2.compute.amazonaws.com United States
pubsub-edge.twitch.tv	34.209.17.11	AMAZON-02 ec2-34-209-17-11.us-west-2.compute.amazonaws.com United States
spectre.twitch.tv	199.9.255.158	TWITCH United States
release.twitch.tv HTTP: Varnish HTTP TECH: varnish	151.101.130.167	FASTLY United States
affiliate.twitch.tv	108.138.64.13	AMAZON-02 server-108-138-64-13.iad12.r.cloudfront.net United States
analytics.m7g.twitch.tv	18.160.46.38	AMAZON-02 server-18-160-46-38.iad55.r.cloudfront.net United States
clock.event-engineering.twitch.tv	18.155.202.21	AMAZON-02 server-18-155-202-21.sfo53.r.cloudfront.net United States
event-panel.event-engineering.twitch.tv HTTP: CloudFront	13.225.63.51	AMAZON-02 server-13-225-63-51.ewr53.r.cloudfront.net United States
ccu.event-engineering.twitch.tv HTTP: CloudFront	65.8.158.71	AMAZON-02 server-65-8-158-71.sfo53.r.cloudfront.net United States
sfmarketing.twitch.tv	13.111.18.27	SALESFORCE ej27.mta.exacttarget.com United States
mta2.sfmarketing.twitch.tv	13.111.97.213	SALESFORCE mta2.sfmarketing.twitch.tv United States
mta.sfmarketing.twitch.tv	13.111.20.163	SALESFORCE mta.sfmarketing.twitch.tv United States
rpg.twitch.tv	52.21.237.158	AMAZON-AES ec2-52-21-237-158.compute-1.amazonaws.com United States
fr.rpg.twitch.tv	52.28.191.151	AMAZON-02 ec2-52-28-191-151.eu-central-1.compute.amazonaws.com Germany
pubsub-edge-darklaunch.twitch.tv HTTP: Kestrel	44.232.134.126	AMAZON-02 ec2-44-232-134-126.us-west-2.compute.amazonaws.com United States
tmi.twitch.tv	52.40.202.120	AMAZON-02 ec2-52-40-202-120.us-west-2.compute.amazonaws.com United States
click.twitch.tv HTTP: awselb/2.0	52.38.233.148	AMAZON-02 ec2-52-38-233-148.us-west-2.compute.amazonaws.com United States
link.twitch.tv HTTP: nginx HTTP TECH: nginx nginx WordPress	67.199.248.13	GOOGLE-CLOUD-PLATFORM cname.bitly.com United States
m.twitch.tv HTTP: Varnish HTTP TECH: varnish	151.101.130.214	FASTLY United States
www.m.twitch.tv	151.101.66.214	FASTLY United States
lg.tv.twitch.tv HTTP: Varnish HTTP TECH: varnish	151.101.194.167	FASTLY United States
dragonfly.twitch.tv	52.26.102.95	AMAZON-02 ec2-52-26-102-95.us-west-2.compute.amazonaws.com United States
o10.recurly.twitch.tv	167.89.64.215	SENDGRID o10.recurly.twitch.tv United States
funny.twitch.tv	127.0.0.1	unknown
canary.twitch.tv HTTP: Varnish HTTP TECH: varnish	151.101.194.167	FASTLY United States
10.canary.twitch.tv HTTP: Varnish HTTP TECH: varnish	151.101.2.167	FASTLY United States
5.antivirus.ads.amarillo.baker.18.10.canary.twitch.tv HTTP: Varnish HTTP TECH: varnish	151.101.194.167	FASTLY United States
discovery.twitch.tv	199.9.253.190	TWITCH United States
e.community.twitch.tv	13.111.18.27	SALESFORCE ej27.mta.exacttarget.com United States
mta.e.community.twitch.tv	13.111.143.194	SALESFORCE mta.e.community.twitch.tv United States
id-canary.twitch.tv	54.191.41.29	AMAZON-02 ec2-54-191-41-29.us-west-2.compute.amazonaws.com United States

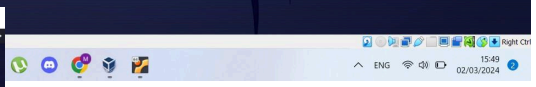
5) Discover and provide information on the organization associated with the website. Look for details such as the organization's name, address, and any publicly available information.

1 - imdb.com

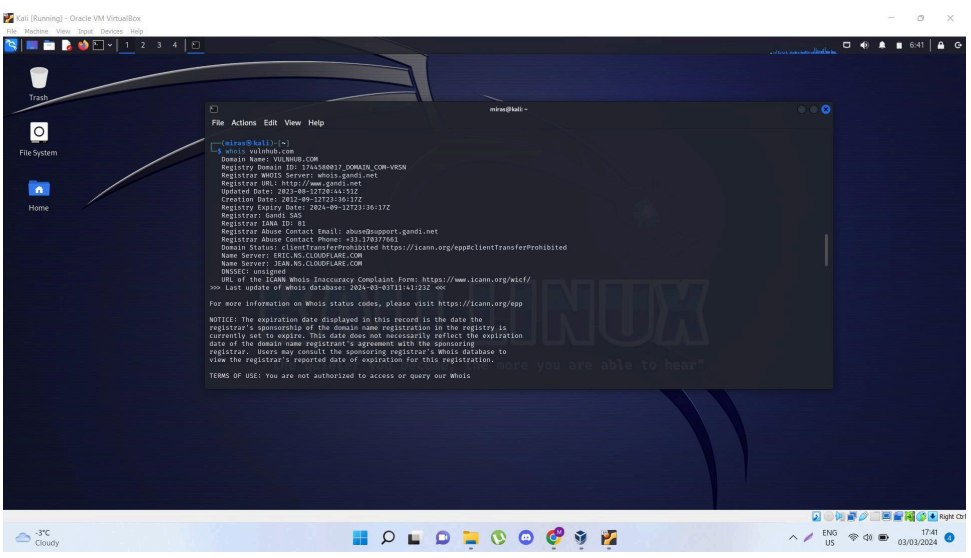




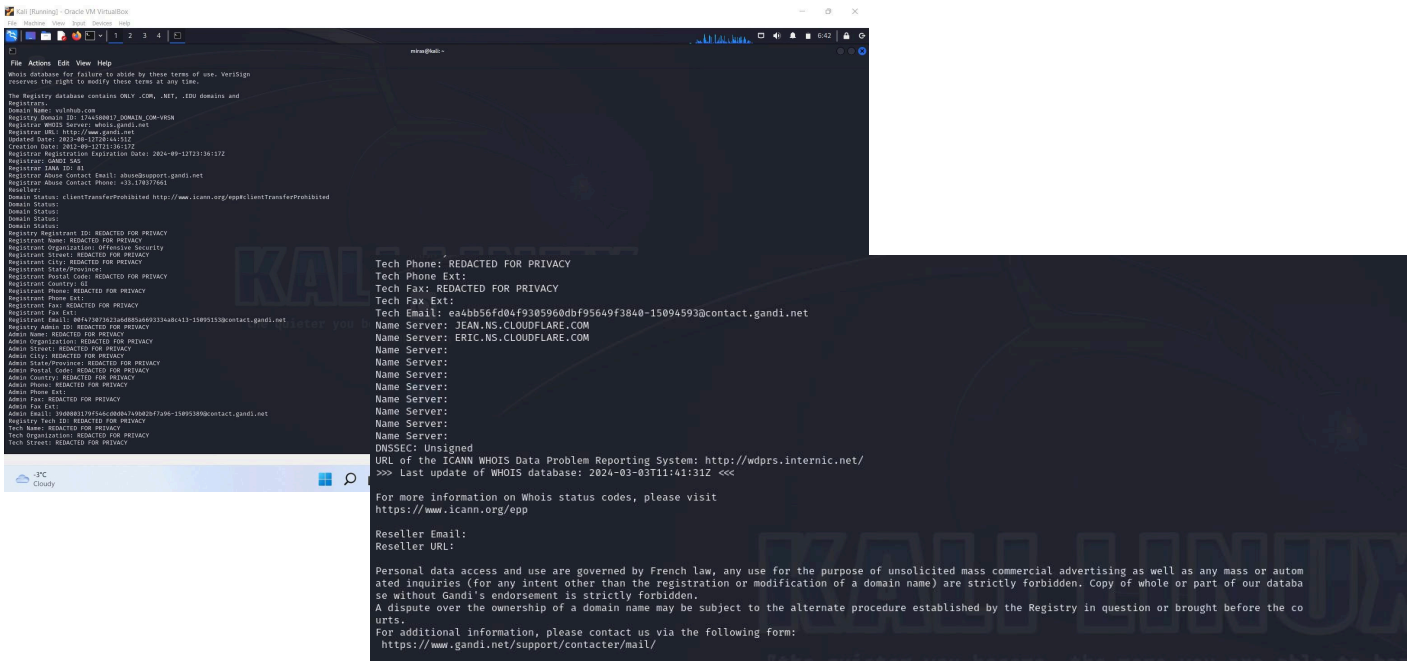




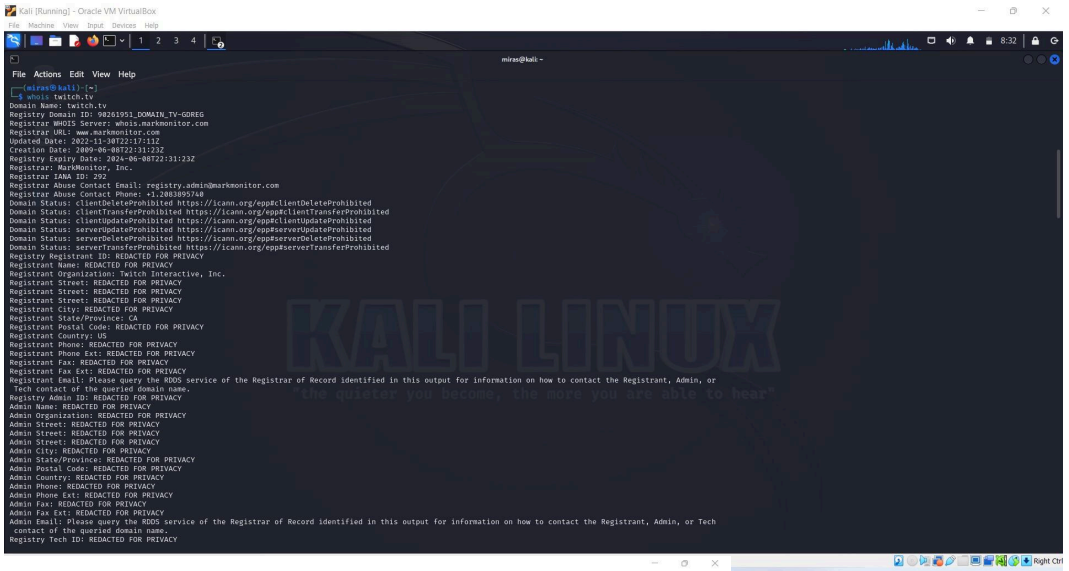

```
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/imdb.com
Admin Organization: IMDb.com, Inc.
Admin State/Province: WA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/imdb.com
Tech Organization: IMDb.com, Inc.
Tech State/Province: WA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/imdb.com
Name Server: ns1.amzndns.com
Name Server: ns1.amzndns.net
Name Server: ns2.amzndns.org
Name Server: ns2.amzndns.net
Name Server: ns1.amzndns.co.uk
Name Server: ns2.amzndns.com
Name Server: ns1.amzndns.org
Name Server: ns2.amzndns.co.uk
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-03-02T09:46:49+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).
```

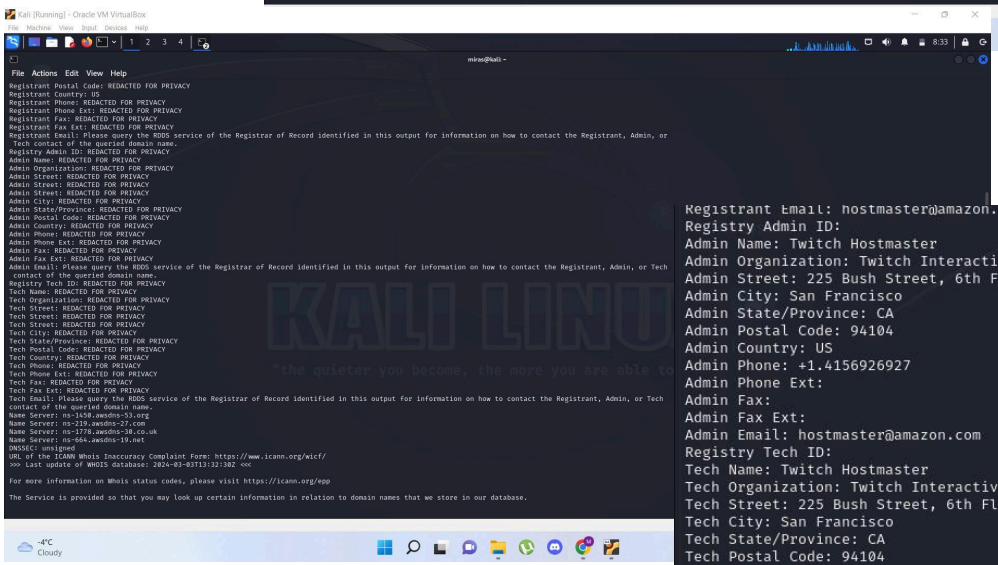


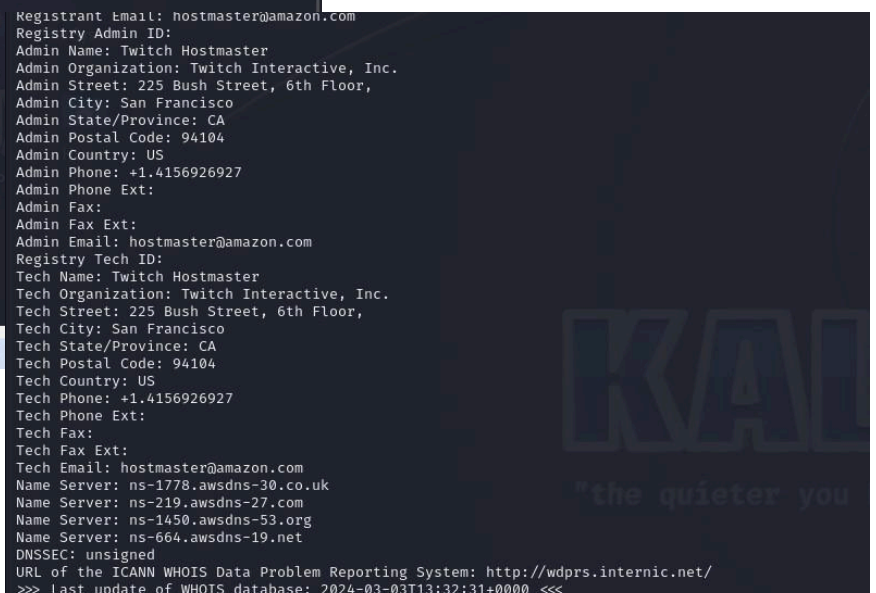
2 - vulnhub.com



3 - twitch.tv

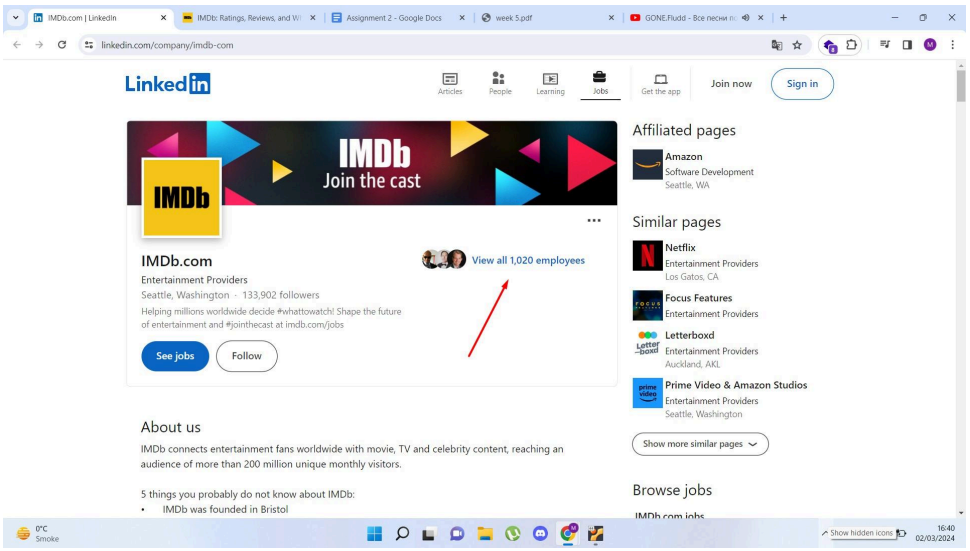


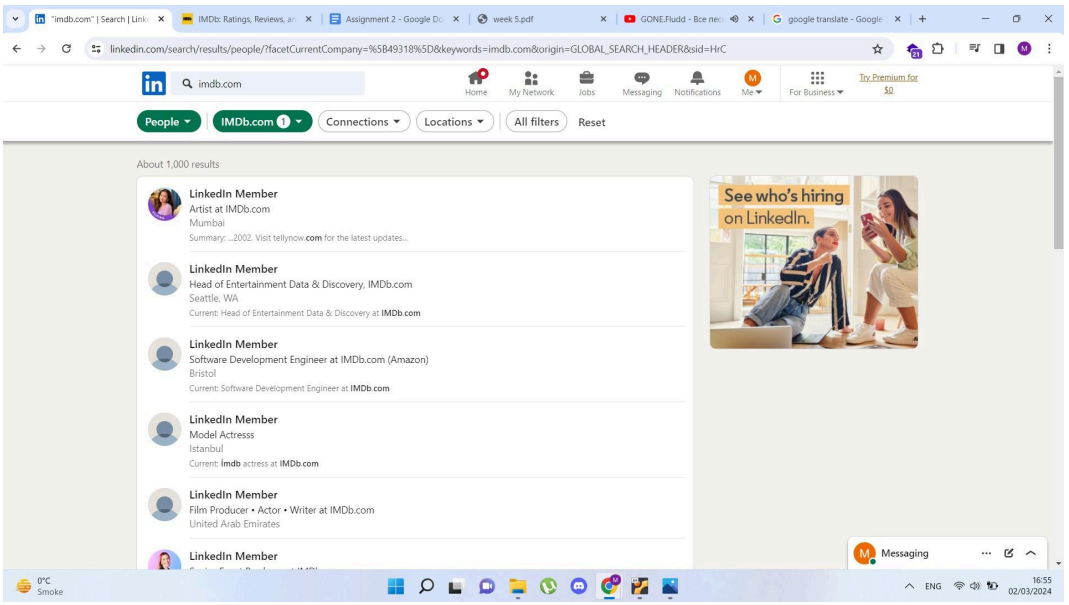


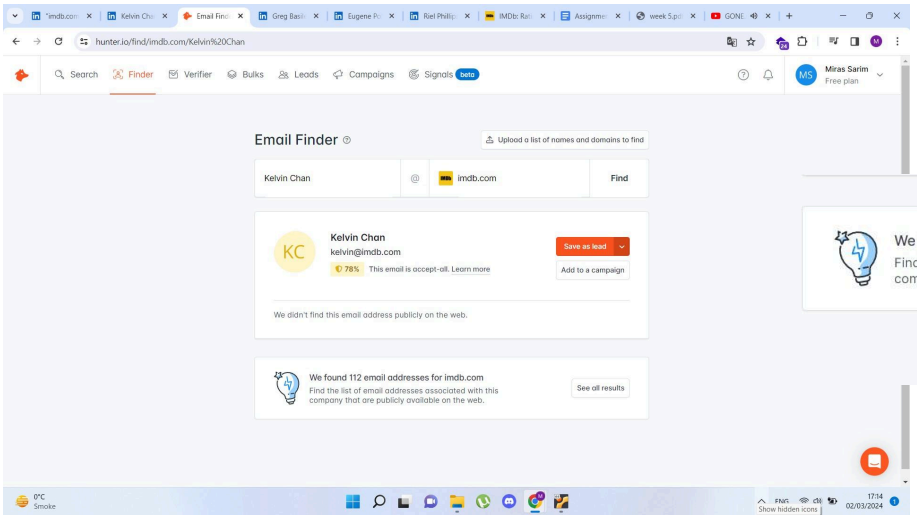


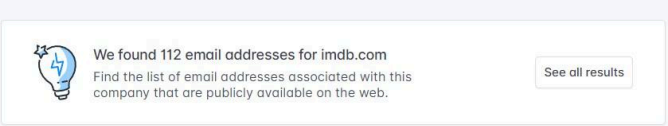
6) Search for a list of employees working in the organization and identify their email addresses

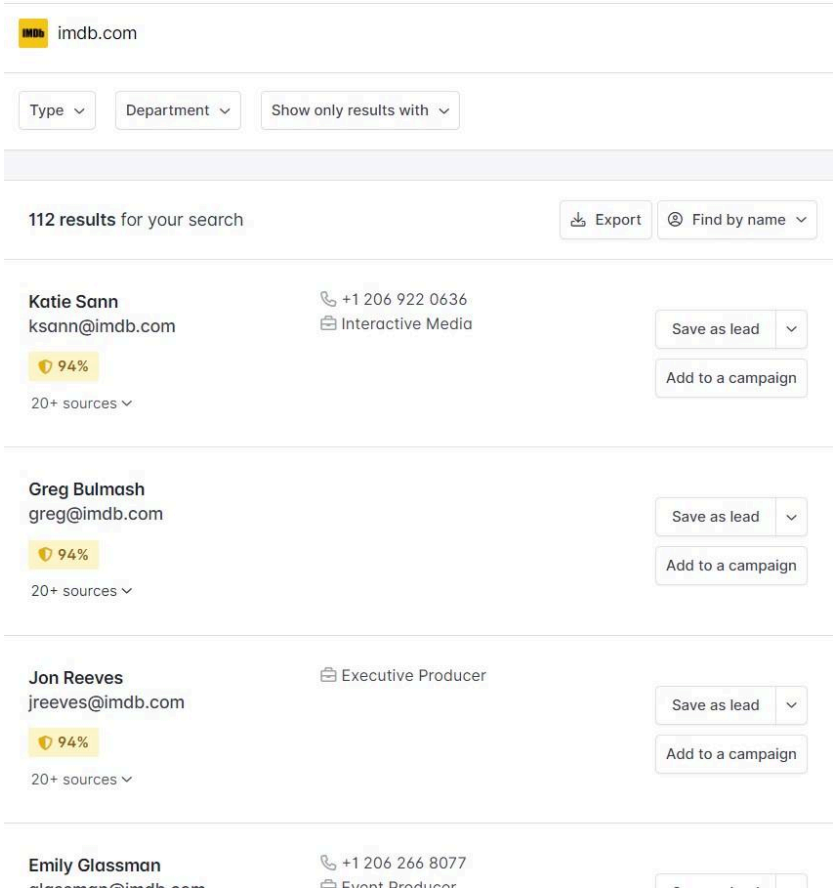
1 - imdb.com



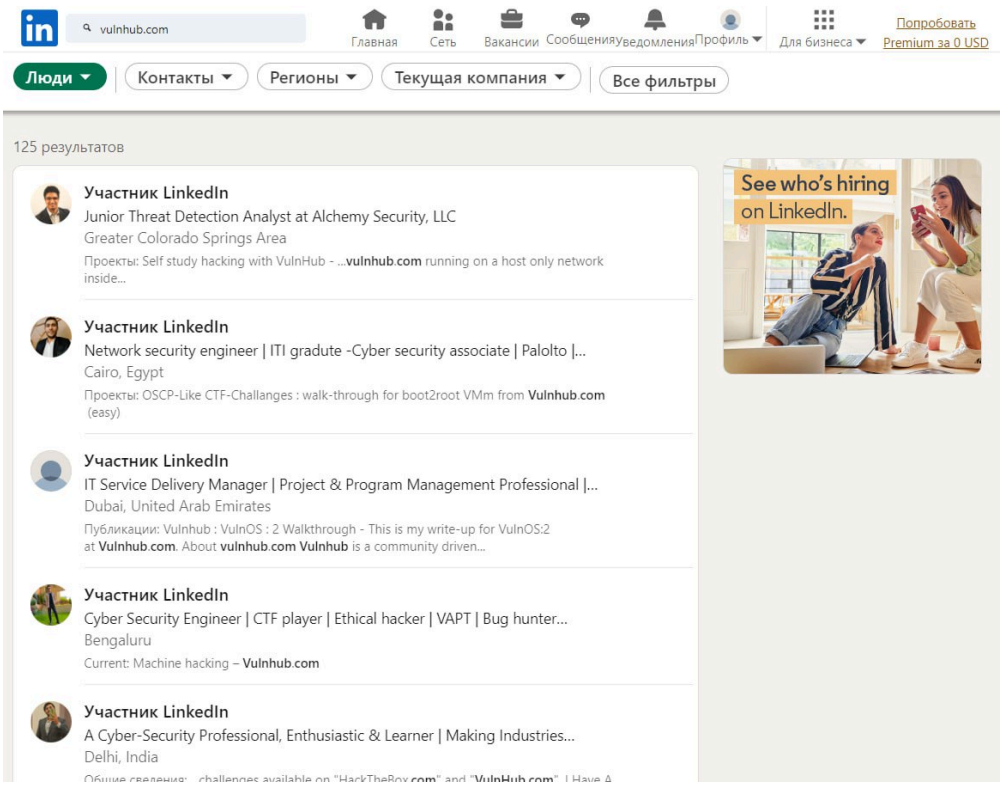


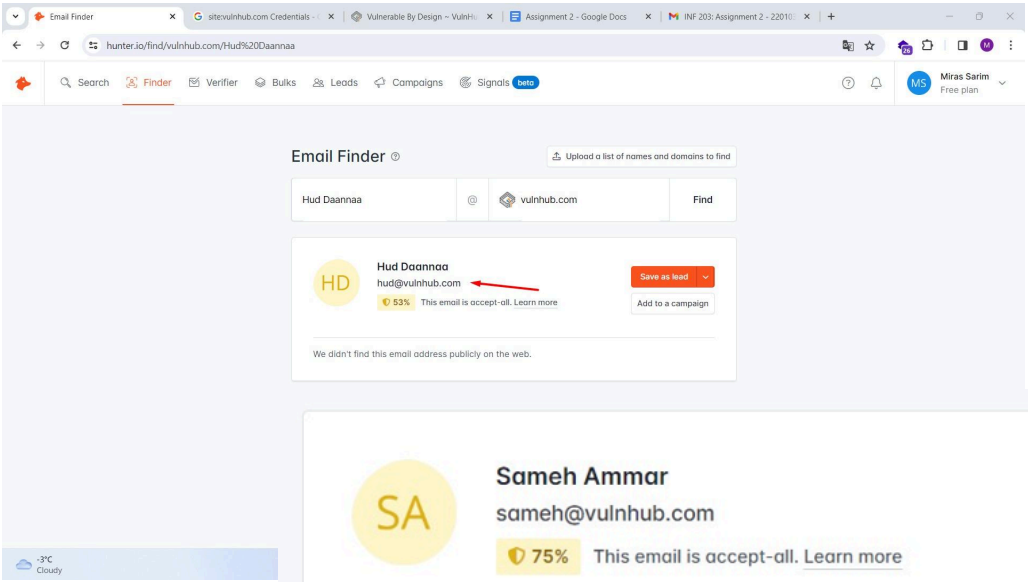


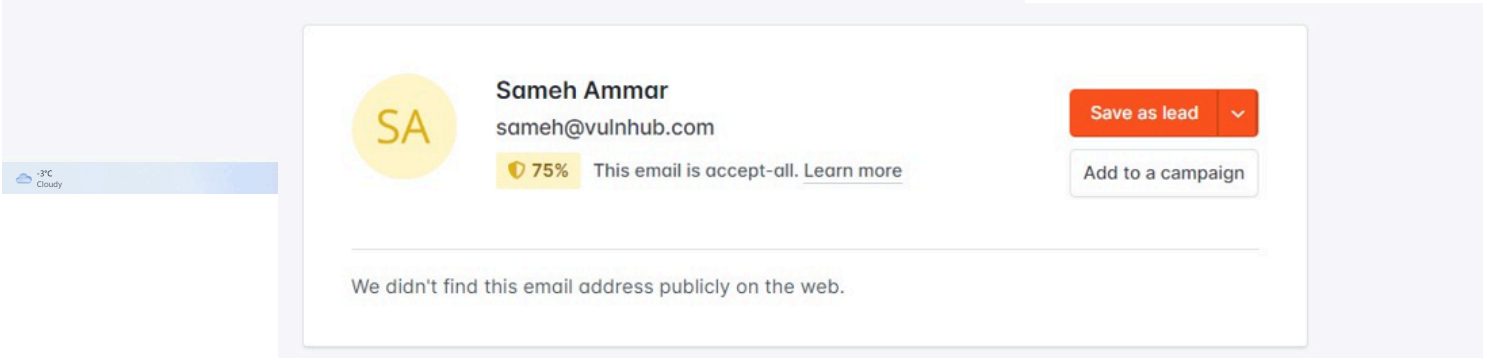




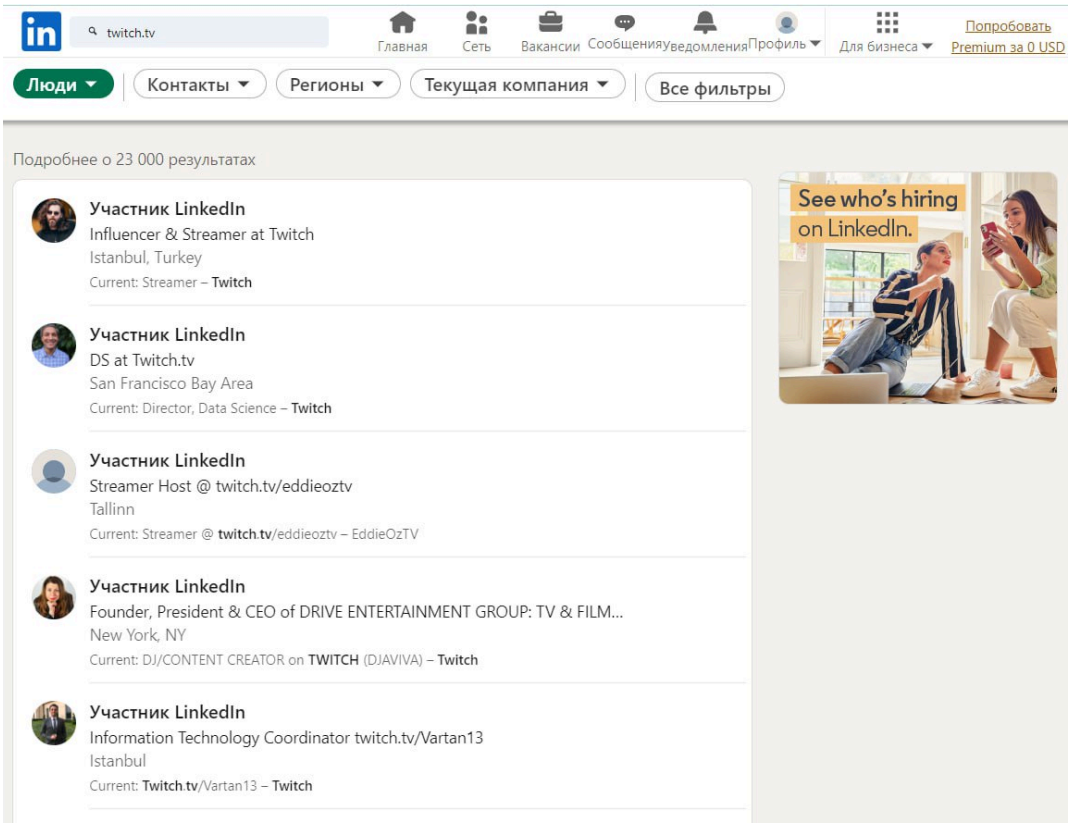
2 - vulnhub.com

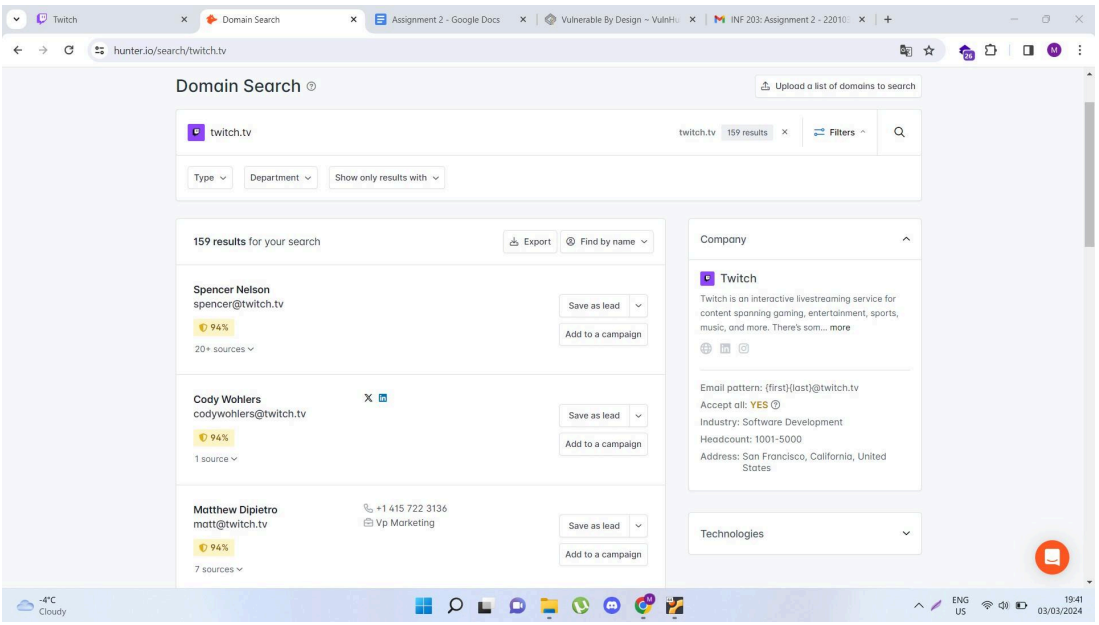






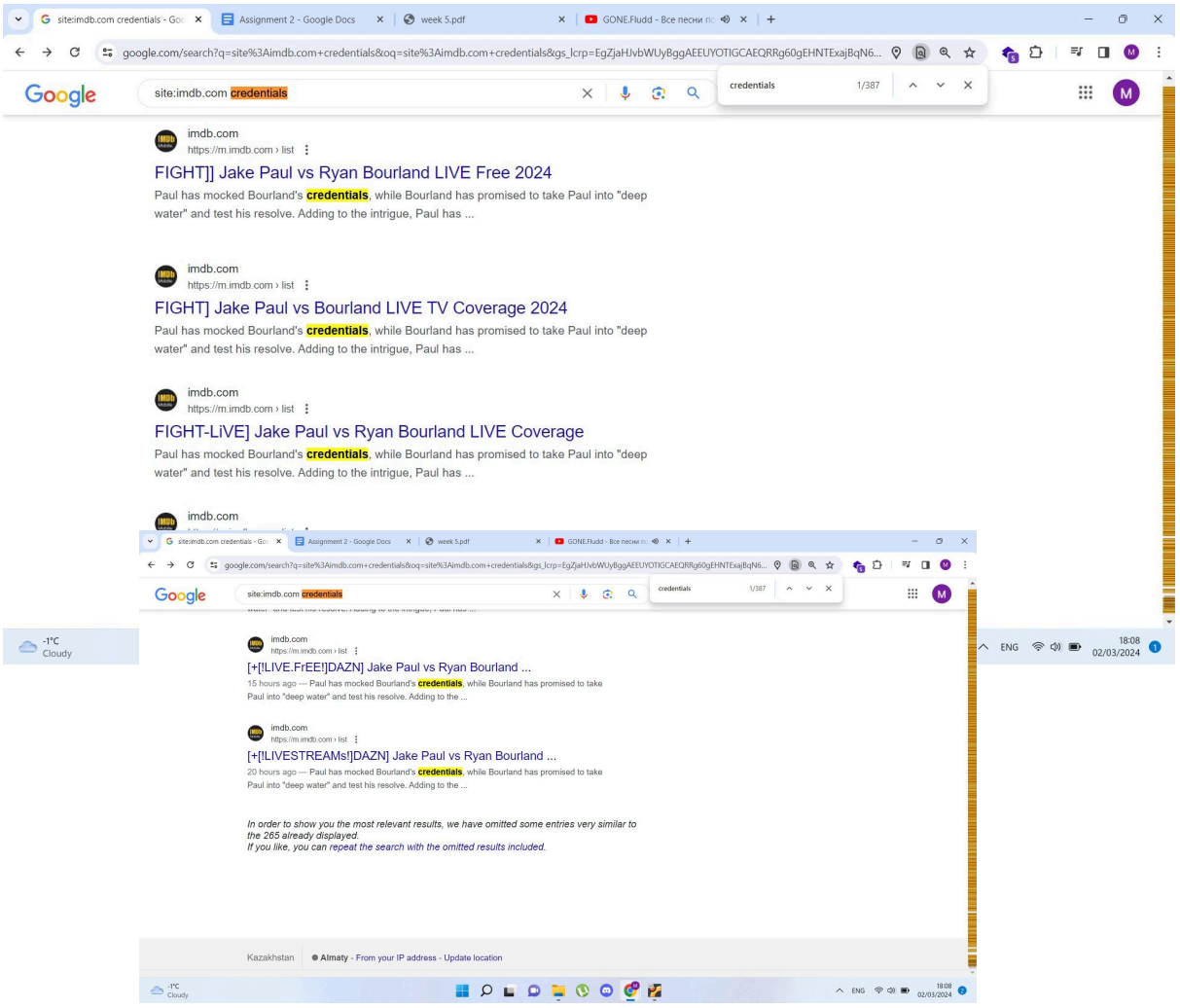
3 - twitch.tv



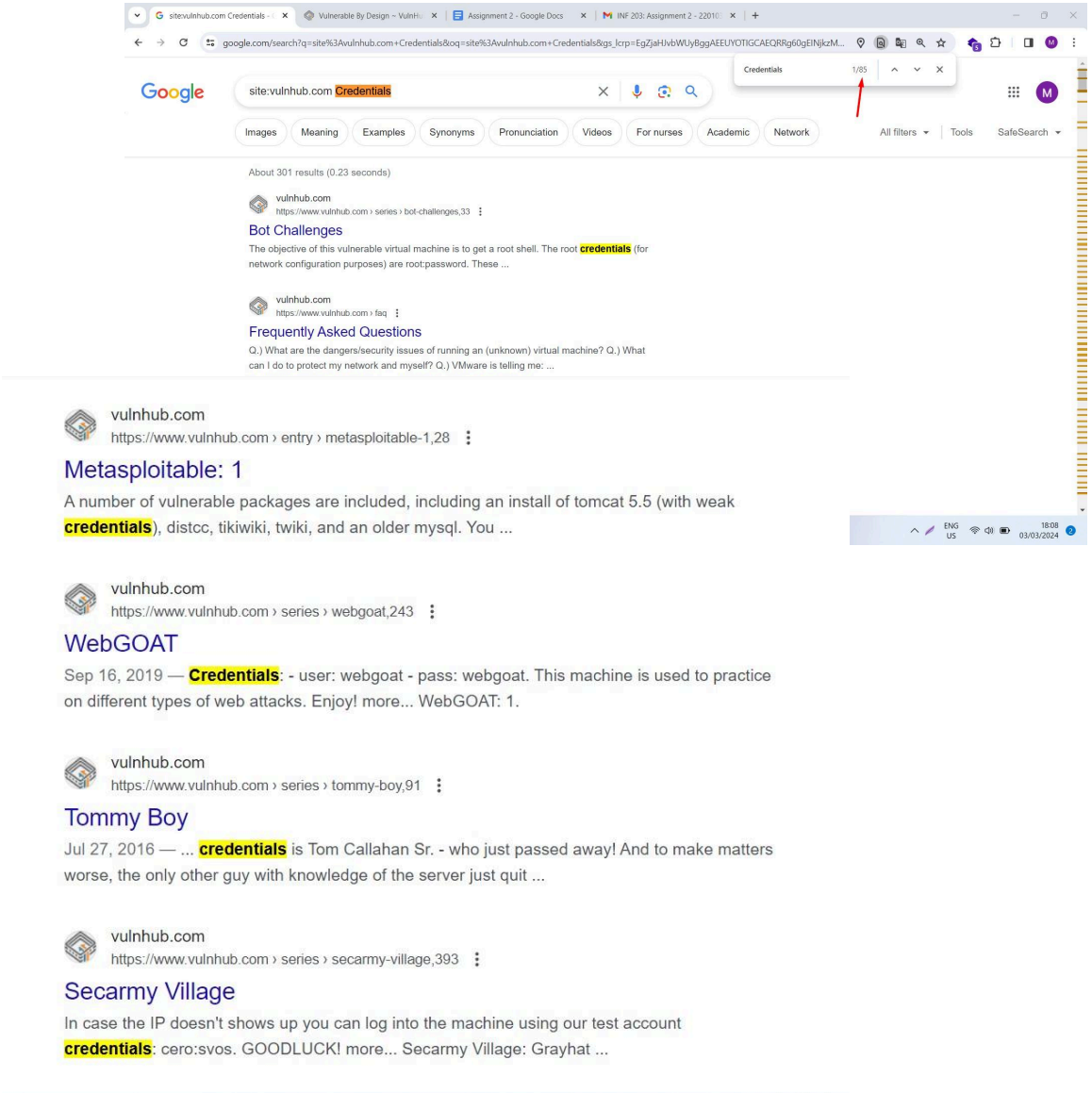


7) Perform a Google search with the site operator to find results containing the word "Credentials" in the text on the target website. Analyze the search results and report the number of instances.

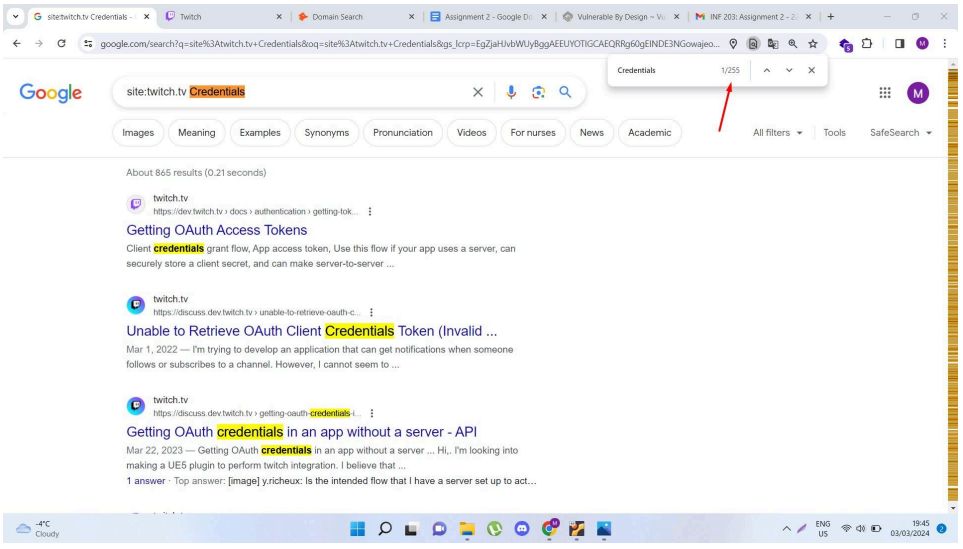
1 - imdb.com (TV Shows, series, films that contains this word in description or in name)



2 - vulnhub.com (offers vulnerable virtual machines for practicing penetration testing, often has "credentials" in their titles or methods.)



3 - twitch.tv (Streamers has nicknames, description or streams that has this word)



twitch.tv
https://link.twitch.tv › ChillhopMusicCreatorProgram

Creators - Chillhop MusicChillhop Music

No, we're only asking for the minimum **credentials** required to read which videos you have uploaded on your YouTube channel so we can monitor if videos that ...

twitch.tv
https://dev.twitch.tv › docs › authentication › getting-tok...

Using OIDC to get OAuth Access Tokens

Feb 3, 2022 — NOTE If you need an app access token, you must use the client **credentials** flow. Discovering supported claims and authorization URIs. To ...

twitch.tv
https://www.twitch.tv › videos

The Safe Room: Responding to Security Events | EP1 - Twitch

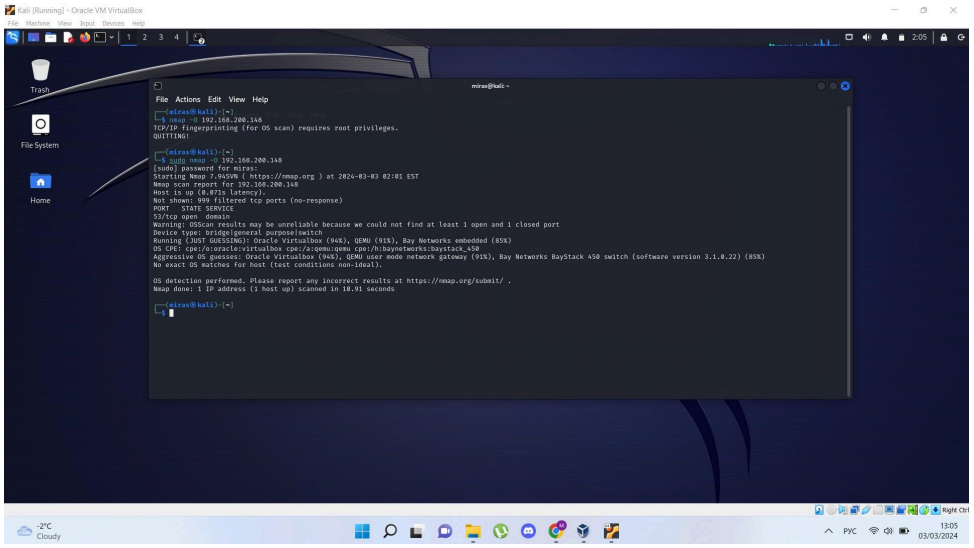
Din webbläsare kan inte spela upp den här videon. AWS. The Safe Room: Responding to Security Events | EP1 | Protecting AWS IAM **credentials**. 46 ...

Twitch · Dec 14, 2021

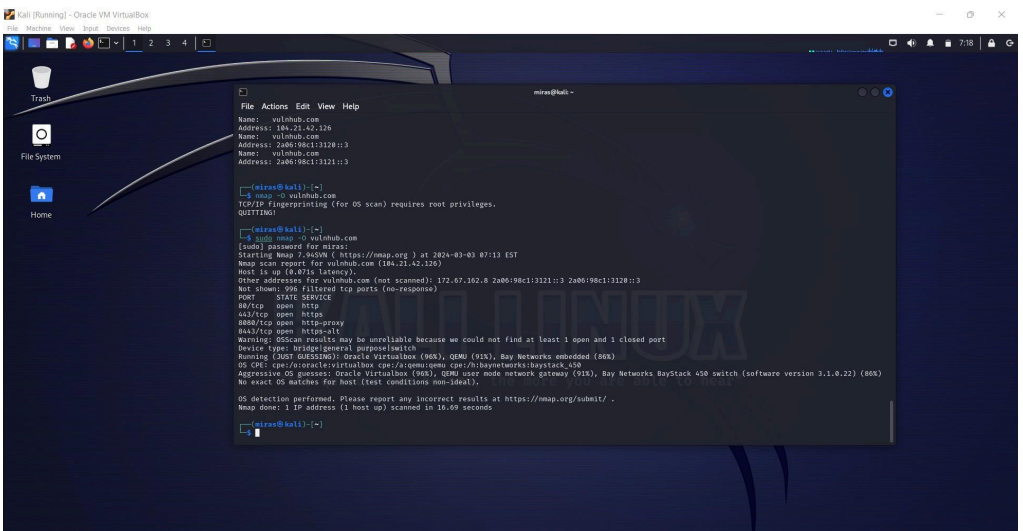
In order to show you the most relevant results, we have omitted some entries very similar to the 222 already displayed.
If you like, you can repeat the search with the omitted results included.

8) Find an operating system that is installed on the server.

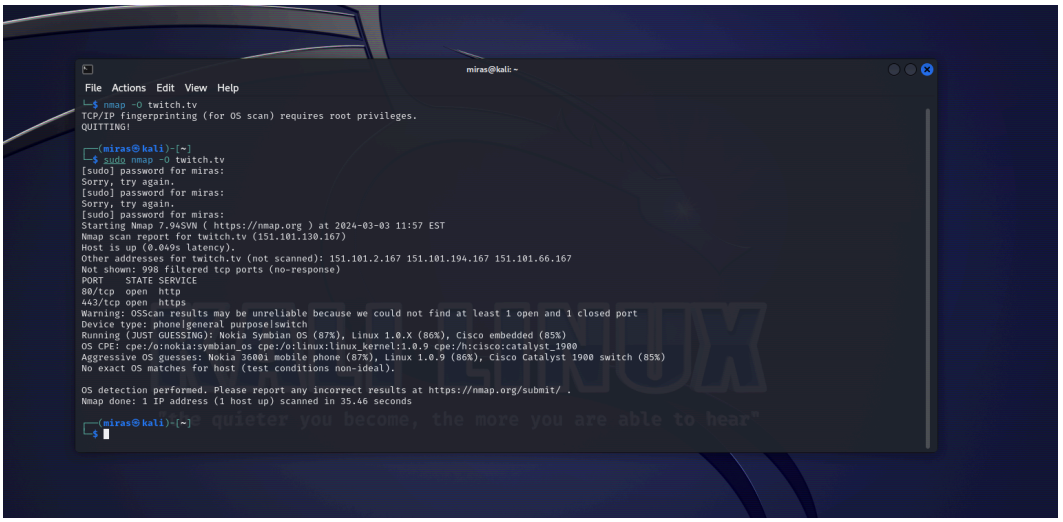
1 - imdb.com



2 - vulnhub.com

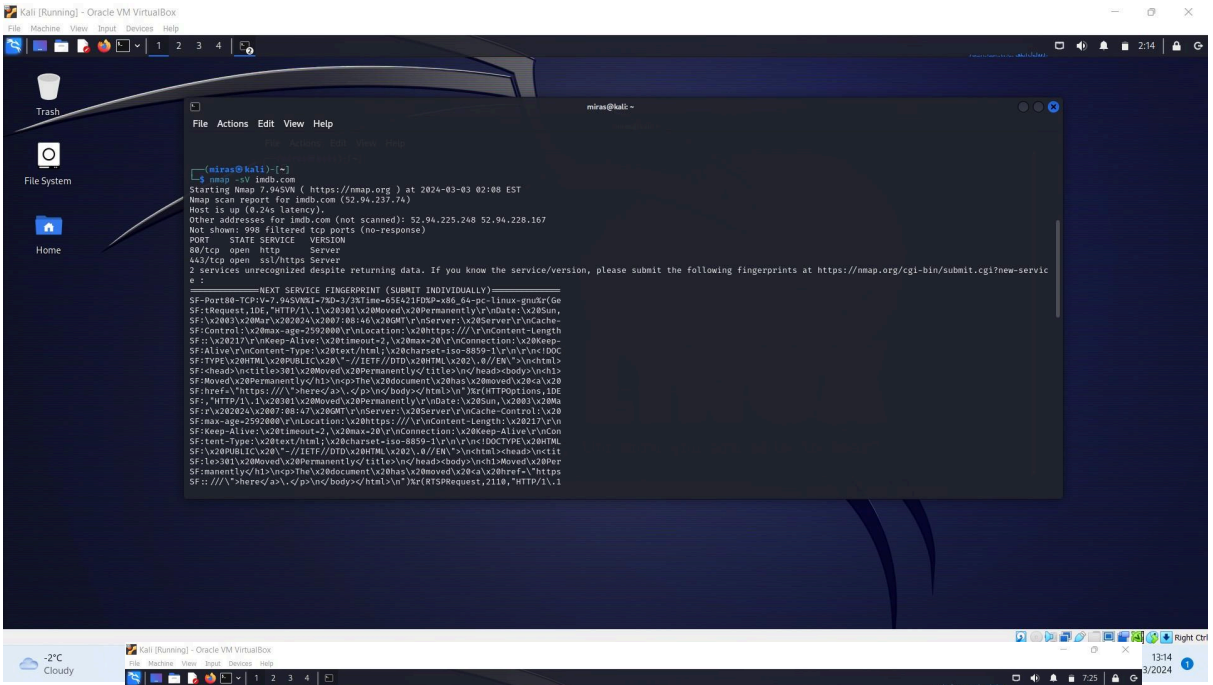


3 - twitch.tv

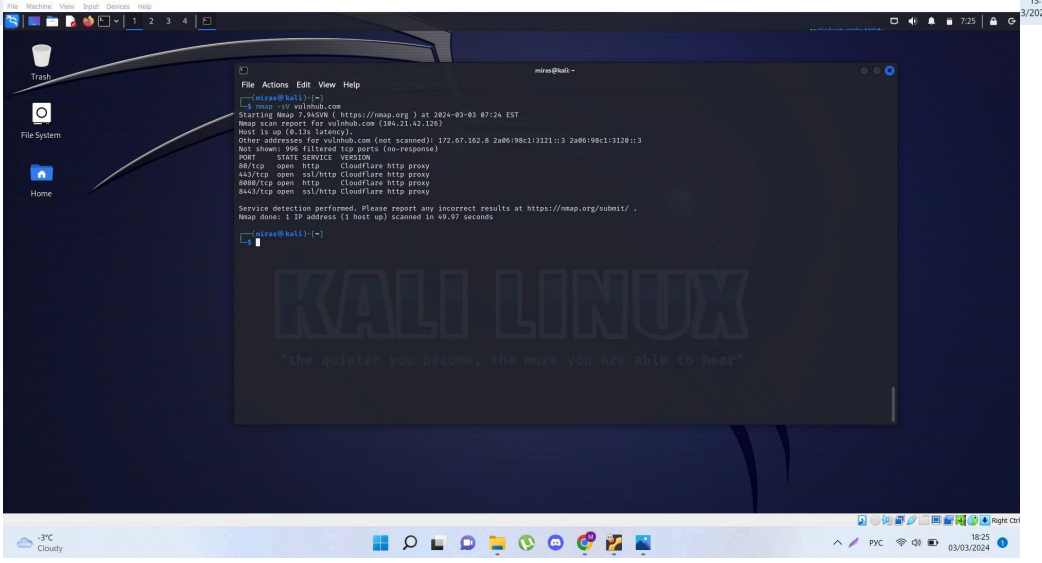


9) Find services that are running on the server. Provide information about port numbers, service names, versions, and so on.

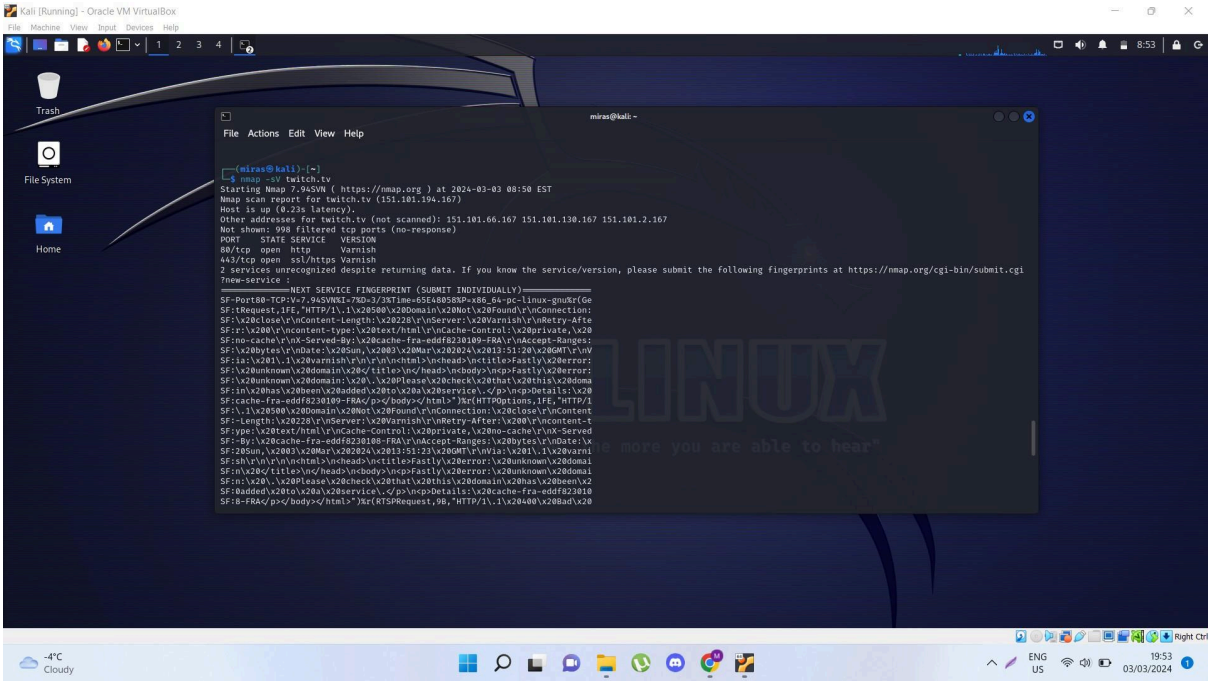
1 - imdb.com



2 - vulnhub.com

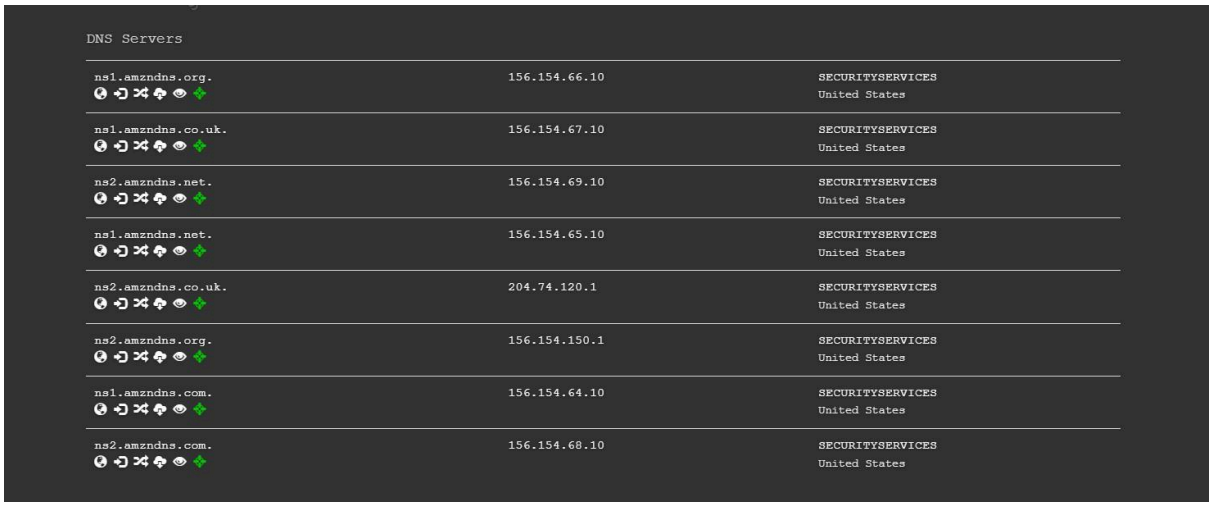


3 - twitch.tv

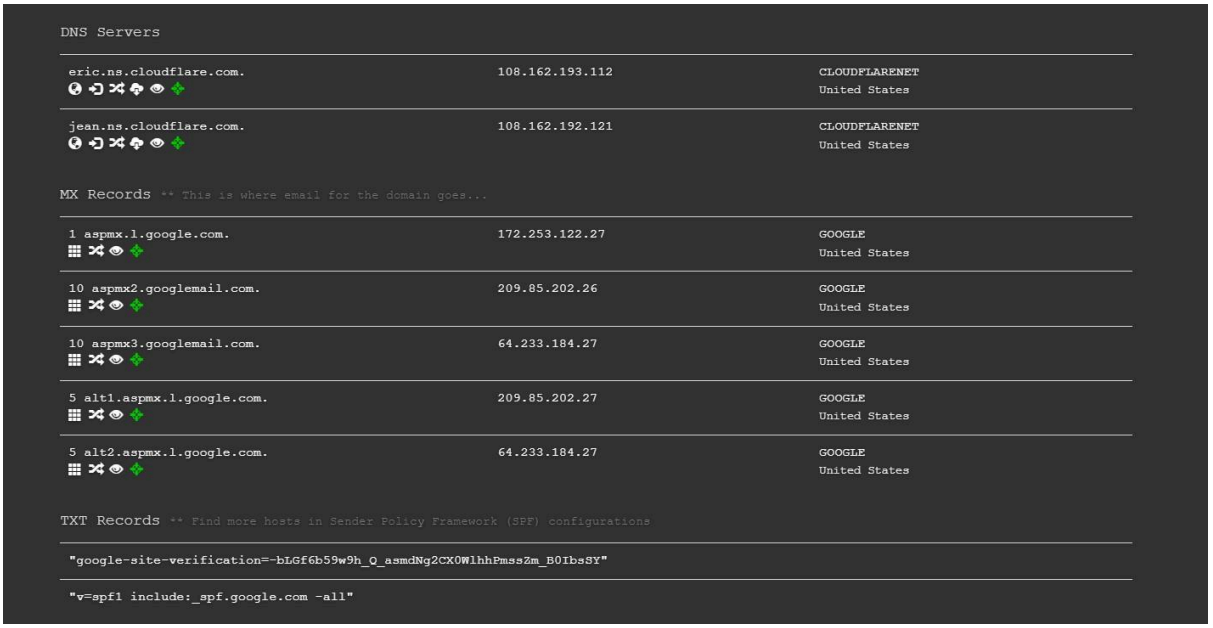


10) Provide information about DNS Servers, MX records, and TXT records related to the domain.

1 - imdb.com **(**Again we are using dnsdumpster.com)



2 - vulnhub.com



DNS Servers

eric.ns.cloudflare.com.	108.162.193.112	CLOUDFLARENET United States
jean.ns.cloudflare.com.	108.162.192.121	CLOUDFLARENET United States

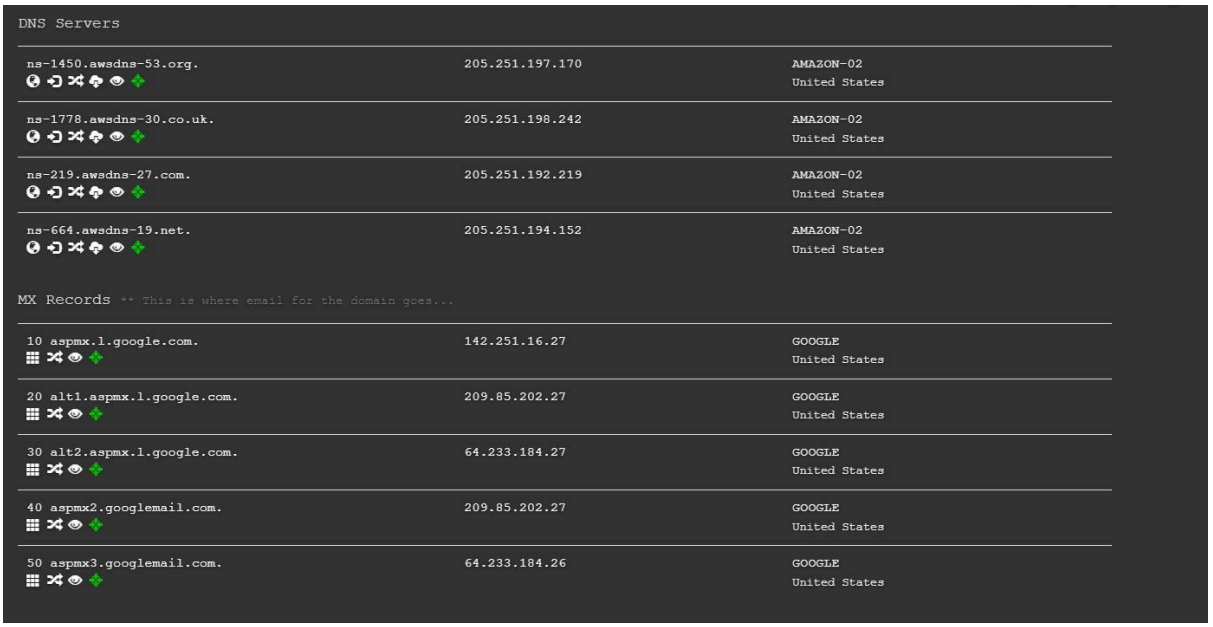
MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com.	172.253.122.27	GOOGLE United States
10 aspmx2.googlemail.com.	209.85.202.26	GOOGLE United States
10 aspmx3.googlemail.com.	64.233.184.27	GOOGLE United States
5 alt1.aspmx.l.google.com.	209.85.202.27	GOOGLE United States
5 alt2.aspmx.l.google.com.	64.233.184.27	GOOGLE United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"google-site-verification=-bLGf6b59w9h_Q_asmdNg2CX0WlhhPmssZm_B0IbsSY"
"v=spf1 include:_spf.google.com -all"

3 - twitch.tv



DNS Servers

ns-1450.awsdns-53.org.	205.251.197.170	AMAZON-02 United States
ns-1778.awsdns-30.co.uk.	205.251.198.242	AMAZON-02 United States
ns-219.awsdns-27.com.	205.251.192.219	AMAZON-02 United States
ns-664.awsdns-19.net.	205.251.194.152	AMAZON-02 United States

MX Records ** This is where email for the domain goes...

10 aspmx.l.google.com.	142.251.16.27	GOOGLE United States
20 alt1.aspmx.l.google.com.	209.85.202.27	GOOGLE United States
30 alt2.aspmx.l.google.com.	64.233.184.27	GOOGLE United States
40 aspmx2.googlemail.com.	209.85.202.27	GOOGLE United States
50 aspmx3.googlemail.com.	64.233.184.26	GOOGLE United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"03vnqw0f74w2ssqpg6vtdpybnnk7v81k"

"MS=ms29920882"

"_globalsign-domain-verification=9UioyPO0_F2Epyd3gGV5_VklXzoibTukD_jkbZPw43"

"_globalsign-domain-verification=PeBo1xAMkWVFOqJ28xB-APP6cLPZNF6oB7m4jy94oR"

"amazonses:103ntJItAHAS8zF3zrp1+RajxRQJ4tlPSC9BB4StgBk="

"amazonses:36386uCaP/zadqoJqgFiBovDfuvRnOQaIdSiMN2ck7I="

"amazonses:E0blpTRNogJgo+NEwz1pCdbiAOW8uziSRCezsgdhTZ8="

"amazonses:TS/Q8uPSq0t+/WbYLWgVUDzblQD3Eg1T1FBxmkfz8kI="

"amazonses:cpm2Dn+xS6T56Iq1KBjzLE3E7OsD2vAoCQIyxcVgp1c="

"amazonses:lZzYXC4khwzoy6SooezLVTpF8e+7/Jh3JMIUYqv0bWI="

"amazonses:n0xA4rjoeQ1tK6vzeRBViDtPhuXpqsnntVALqWAfEz0="

"amazonses:q1VqNqptpdPoDMi8EixEYsLNRMP1pSxGIY3uOpUdDHQ="

"amazonses:wzbVRObrJcHqXdo623myecXiqm4USLX3kIgSKymaVso="

"atlassian-domain-verification=PR1VWTs0H2FZsDQVhpCAAxSgaKScDpfZdEiDf46abvU1/BTE2BMDRWCXxHYAWFRa"

"bugcrowd-verification=4cb12e80d1cc53286a15726ee4bf8f6e"

"cisco-ci-domain-verification=132cb07ebad7bda1f2d4659730b12d115c80a95b6c4e5303a010f3edef248906"

"docusign=79f74da0-0f98-4cdb-b2d3-93871ea127c8"

"google-site-verification=9rDIUbekFpQoTOIBeCYKmEbmngpR6Dp9nJ7ZqLBBwOE"

"google-site-verification=hDc28WSCJ_PZVKa2N6OVyVvD2UqCbxUX81mmBP8QJn0"

"google-site-verification=xYplJj114xfWi8VIM2NFWQUeIbrKUg9achbQ5W4AYJA"

"sending_domain1020022=834b5b18e26655468c764e5279df6460ed66057be1d8c0684722b8c589b35add"

"sprig-site-verification=p7Xa5X9lnBvzD3plB6lcrXfhabY2uX3NAwyEGPm4C98"

"stripe-verification=98fd69ef9979b0dcdc41fc6ea416633b9cd2e008a989b1c64732897a272bb804"

"twilio-domain-verification=7471ef203449152cfc7ec9a3d518a8a2"

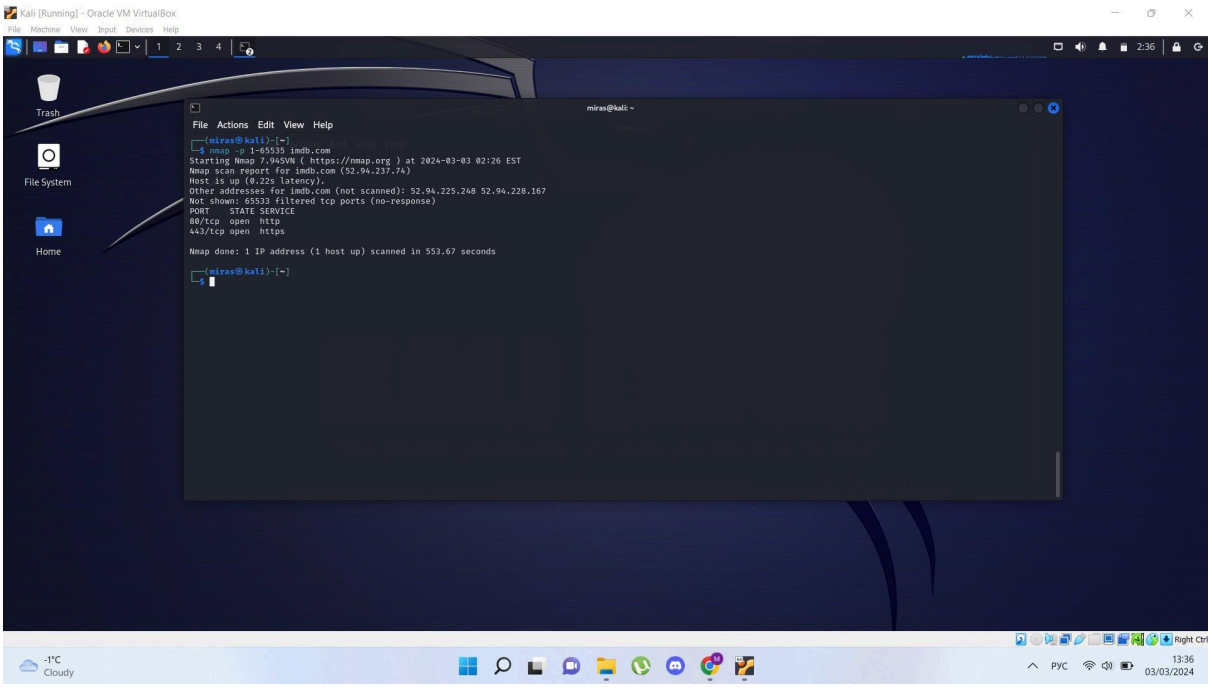
"uber-domain-verification=18c3e151-508f-477d-87fb-23e876237df1"

"v=spf1 include:_spf.google.com include:amazonses.com include:spf.mtasv.net include:mail.zendesk.com include:_spf.twitch.tv include:aspmx.pardot.com a mx -all"

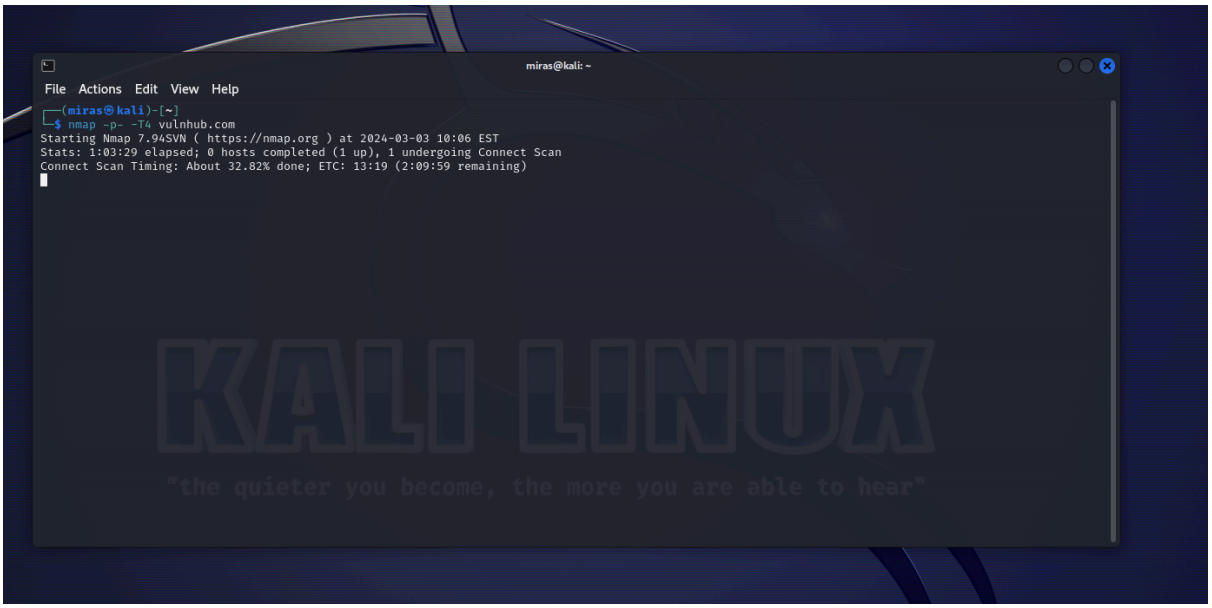
11) Perform scanning of all 65,535 ports on the server.

Nmap is a network scanning tool used to discover hosts and services on computer networks.

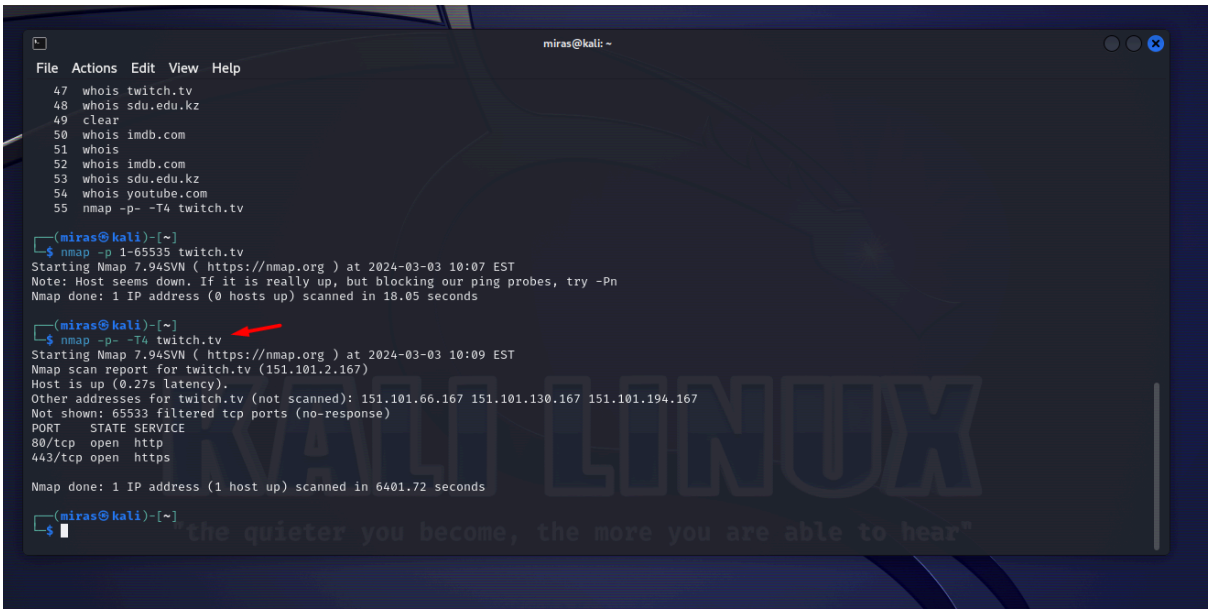
1



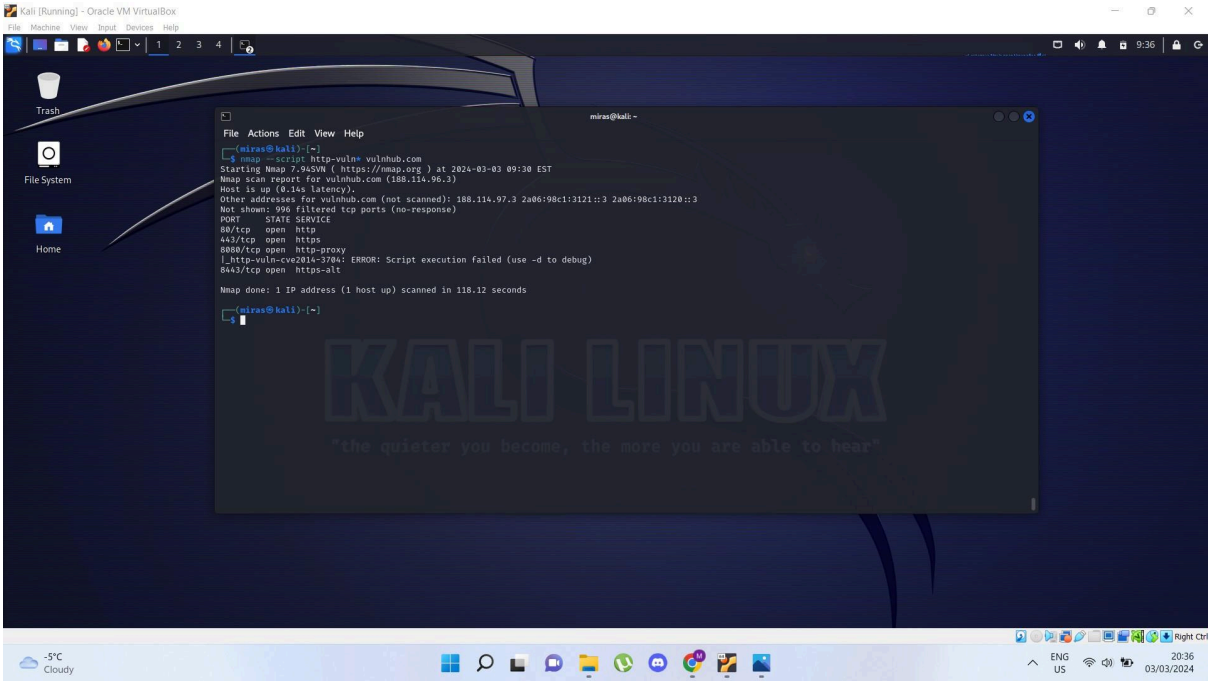
2

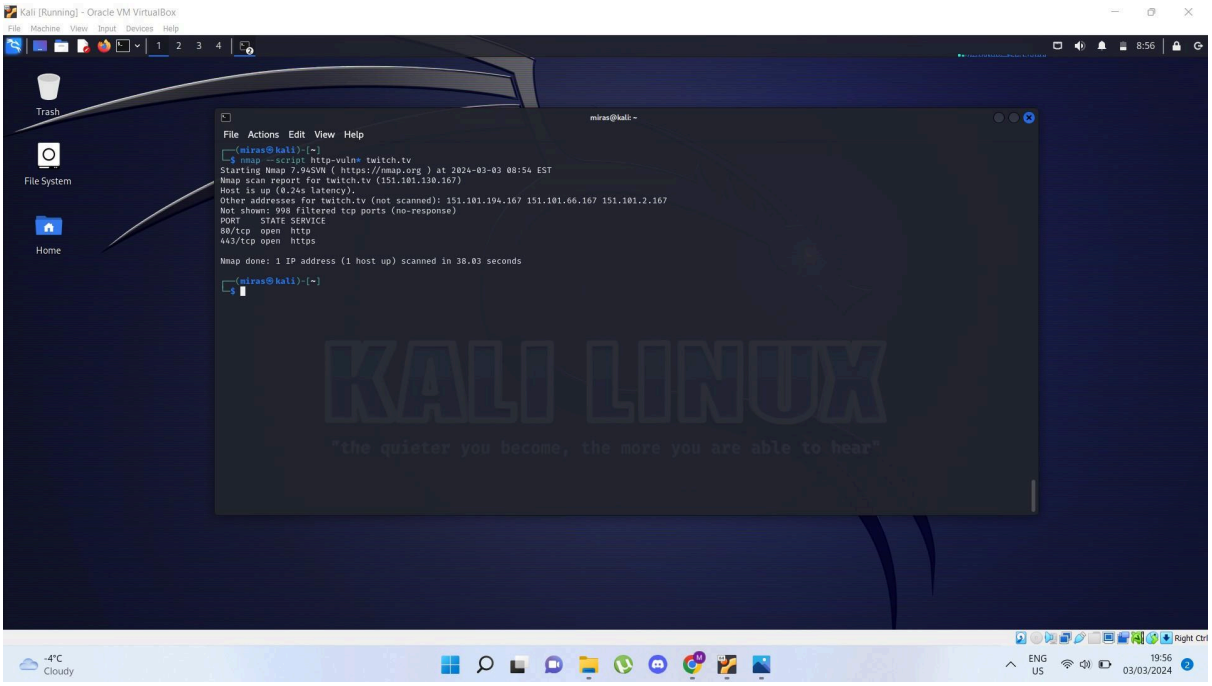


3

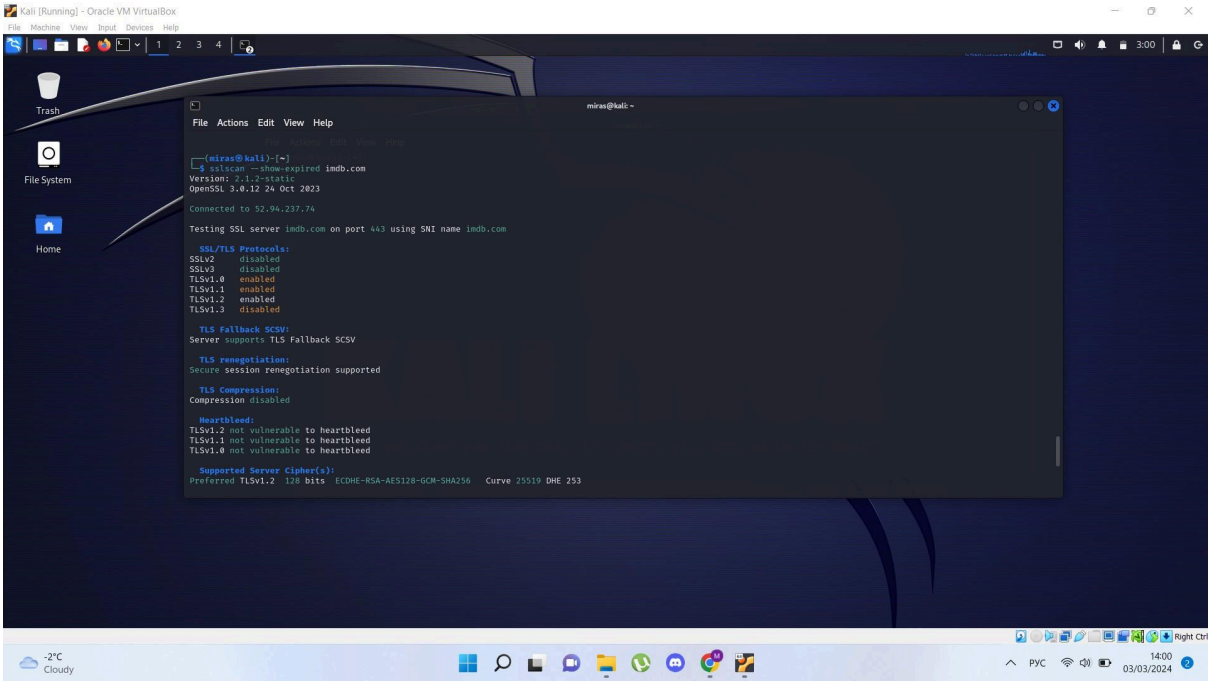


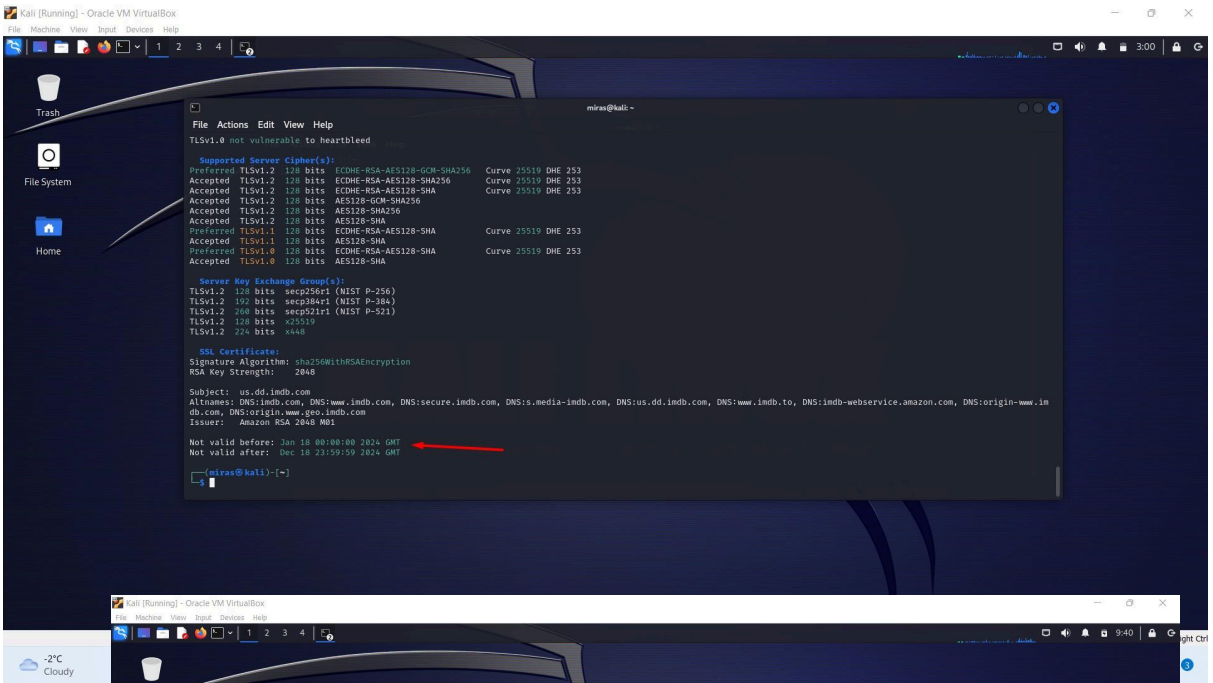
12) Find possible vulnerabilities related to HTTP using NSE.

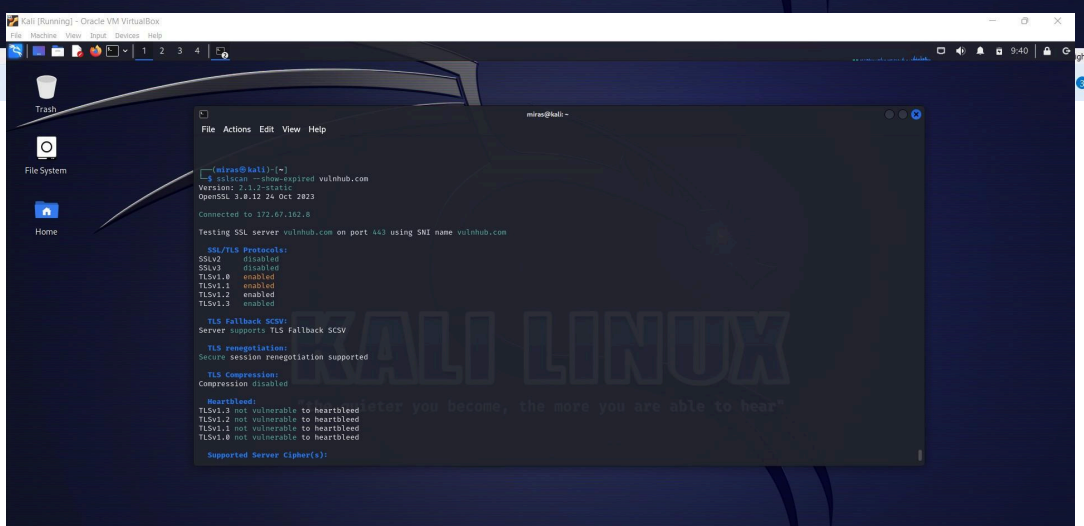

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
miras@kali: ~
File Actions Edit View Help
┌──(miras㉿kali)-[~]
└─$ nmap --script http-vuln* vulnhub.com
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-03 09:30 EST
Nmap scan report for vulnhub.com (188.114.96.3)
Host is up (0.14s latency).
Other addresses for vulnhub.com (not scanned): 188.114.97.3 2a06:98c1:3121::3 2a06:98c1:3120::3
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
8443/tcp open https-alt
Nmap done: 1 IP address (1 host up) scanned in 118.12 seconds
┌──(miras㉿kali)-[~]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl
-5°C
Cloudy
ENG
US
20:36
03/03/2024

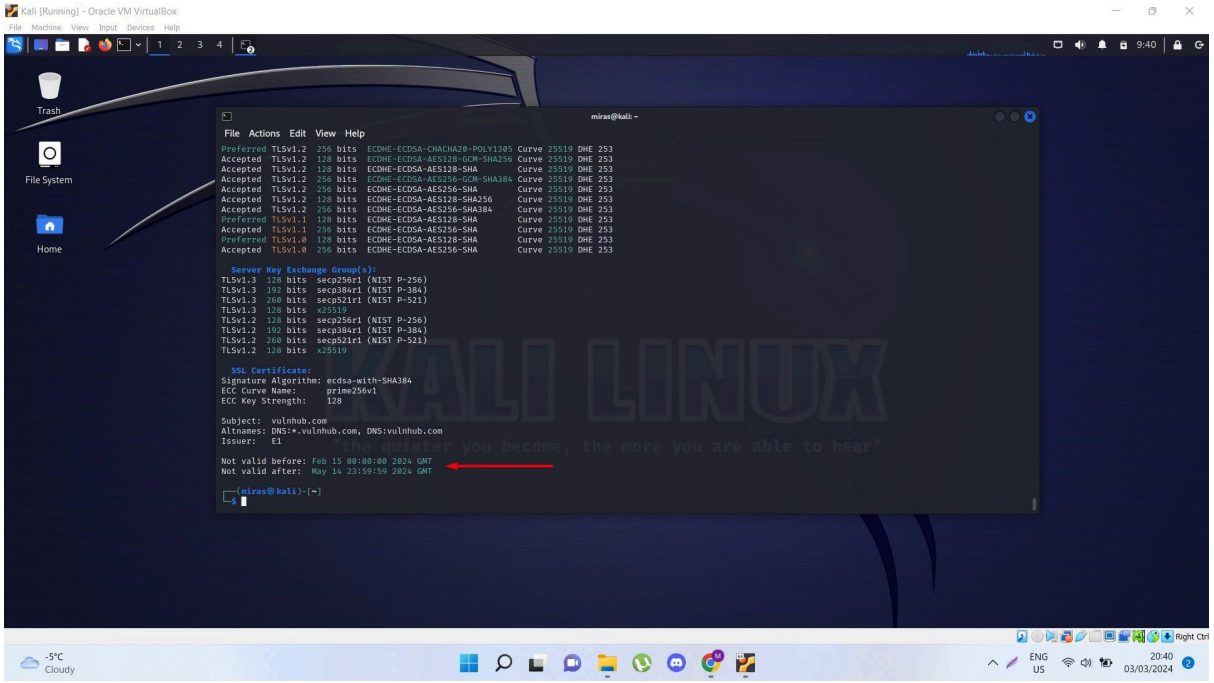

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
miras@kali: ~
File Actions Edit View Help
┌──(miras㉿kali)-[~]
└─$ nmap --script http-vuln* twitch.tv
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-03 08:54 EST
Nmap scan report for twitch.tv (151.101.130.167)
Host is up (0.24s latency).
Other addresses for twitch.tv (not scanned): 151.101.194.167 151.101.66.167 151.101.2.167
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 38.03 seconds
┌──(miras㉿kali)-[~]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl
-4°C
Cloudy
ENG
US
19:56
03/03/2024

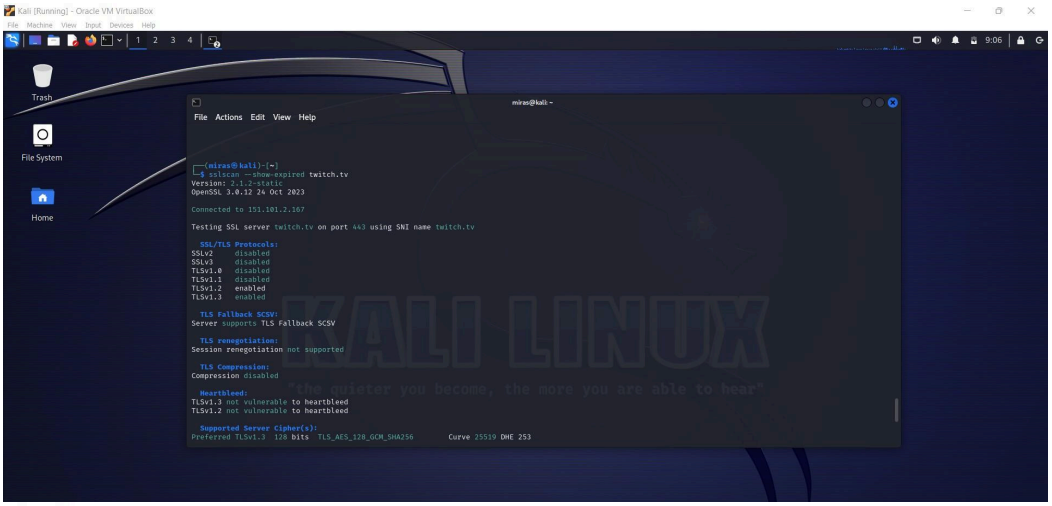
13) Find expired SSL certificates of domains and subdomains.

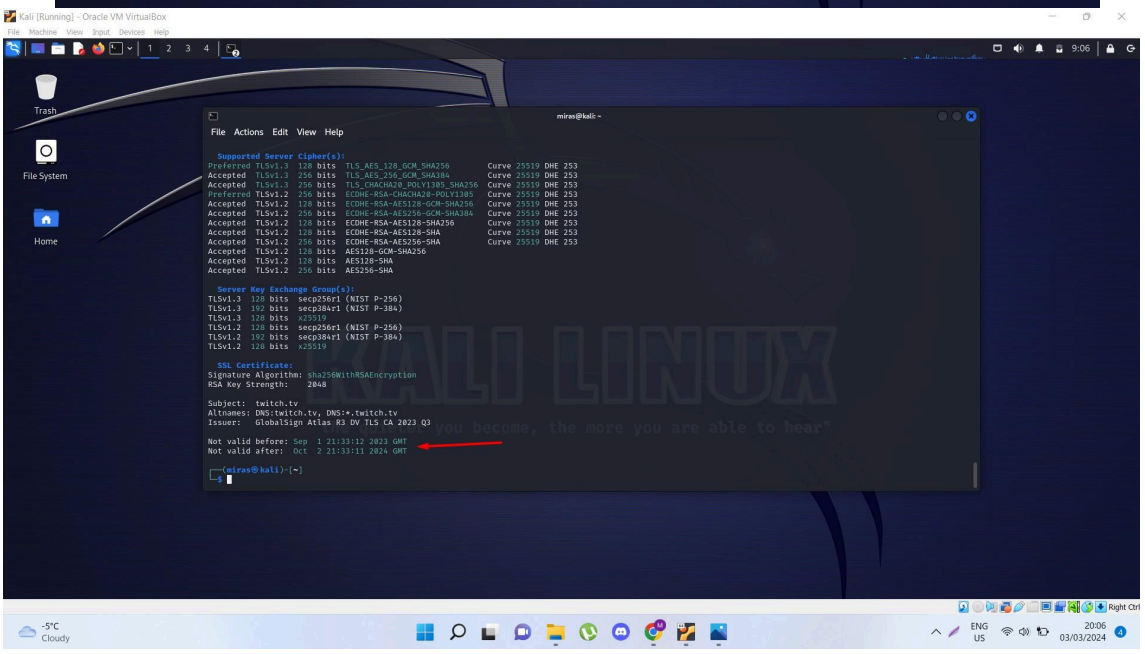






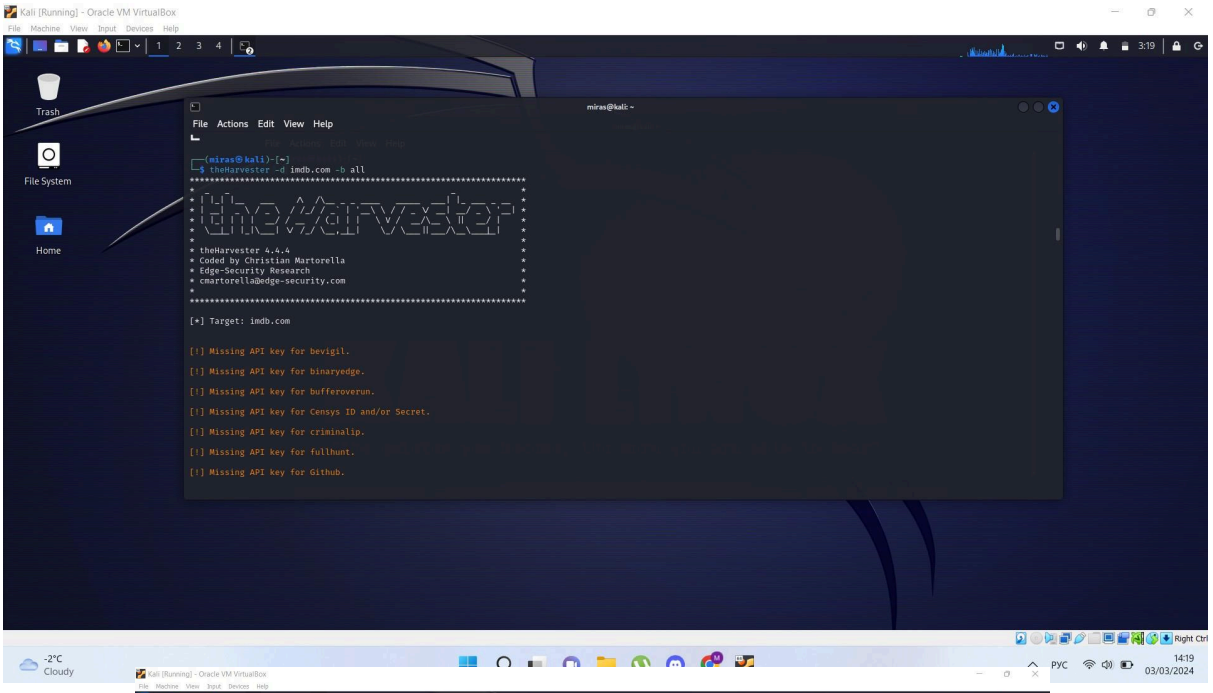

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
miras@kali: ~
File Actions Edit View Help
Preferred TLSv1.2 256 bits ECDHE-ECDSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-SHA Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-SHA384 Curve 25519 DHE 253
Preferred TLSv1.1 128 bits ECDHE-ECDSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.1 256 bits ECDHE-ECDSA-AES256-SHA Curve 25519 DHE 253
Preferred TLSv1.0 128 bits ECDHE-ECDSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.0 256 bits ECDHE-ECDSA-AES256-SHA Curve 25519 DHE 253
Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519
SSL Certificate:
Signature Algorithm: ecdsa-with-SHA384
ECC Curve Name: prime256v1
ECC Key Strength: 128
Subject: vulnhub.com
Altnames: DNS:*.vulnhub.com, DNS:vulnhub.com
Issuer: E1
Not valid before: Feb 15 00:00:00 2024 GMT
Not valid after: May 14 23:59:59 2024 GMT
(miras㉿kali)-[~]
"the quieter you become, the more you are able to hear"
Right Ctrl
-5°C
Cloudy
ENG
US
20:40
03/03/2024

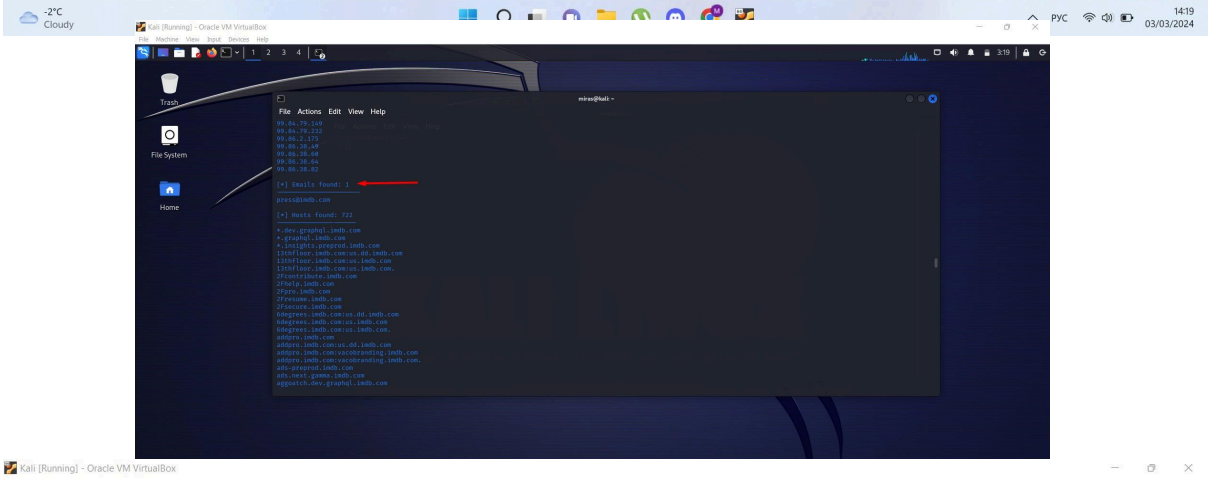

Kali [Running] - Oracle VM VirtualBox
Trash
File System
Home
miras@kali: ~
File Actions Edit View Help
(miras㉿kali)-[~]
$ sslscan --show-expired twitch.tv
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023
Connected to 151.101.2.167
Testing SSL server twitch.tv on port 443 using SNI name twitch.tv
SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 enabled
TLSv1.3 enabled
TLS Fallback SCSV:
Server supports TLS Fallback SCSV
TLS renegotiation:
Session renegotiation not supported
TLS Compression:
Compression disabled
Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed
Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
"the quieter you become, the more you are able to hear"

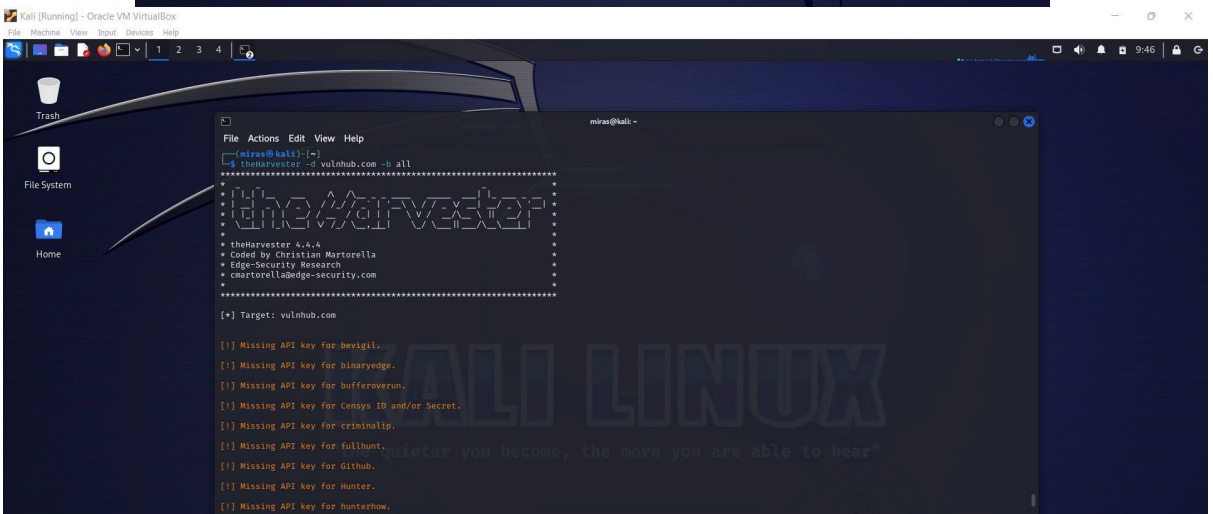

Kali [Running] - Oracle VM VirtualBox
Trash
File System
Home
miras@kali: ~
File Actions Edit View Help
Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 256 bits AES256-SHA
Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 128 bits x25519
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048
Subject: twitch.tv
Altnames: DNS:twitch.tv, DNS:*.twitch.tv
Issuer: GlobalSign Atlas R3 DV TLS CA 2023 Q3
Not valid before: Sep 1 21:33:12 2023 GMT
Not valid after: Oct 2 21:33:11 2024 GMT
(miras㉿kali)-[~]
"the quieter you become, the more you are able to hear"
Right Ctrl
-5°C
Cloudy
ENG
US
20:06
03/03/2024

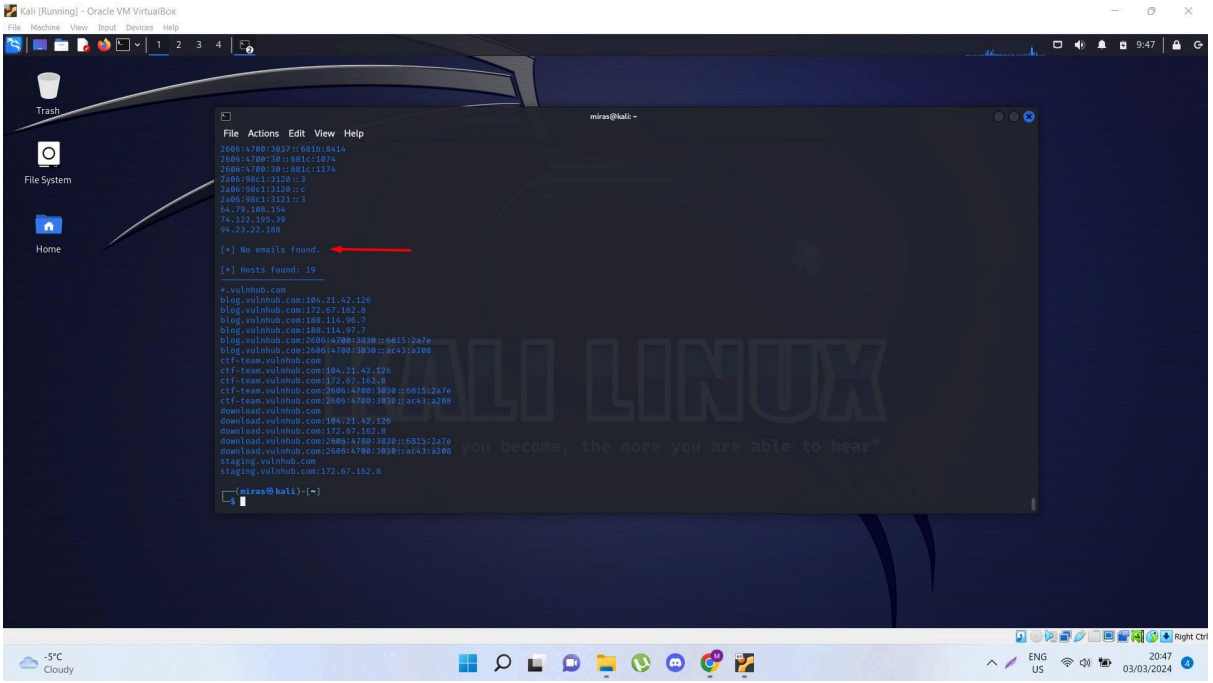
14) Find all emails that are available in the web content of the website.

TheHarvester is a tool used for gathering email accounts, subdomains, hosts, employee names, and open ports from public sources.

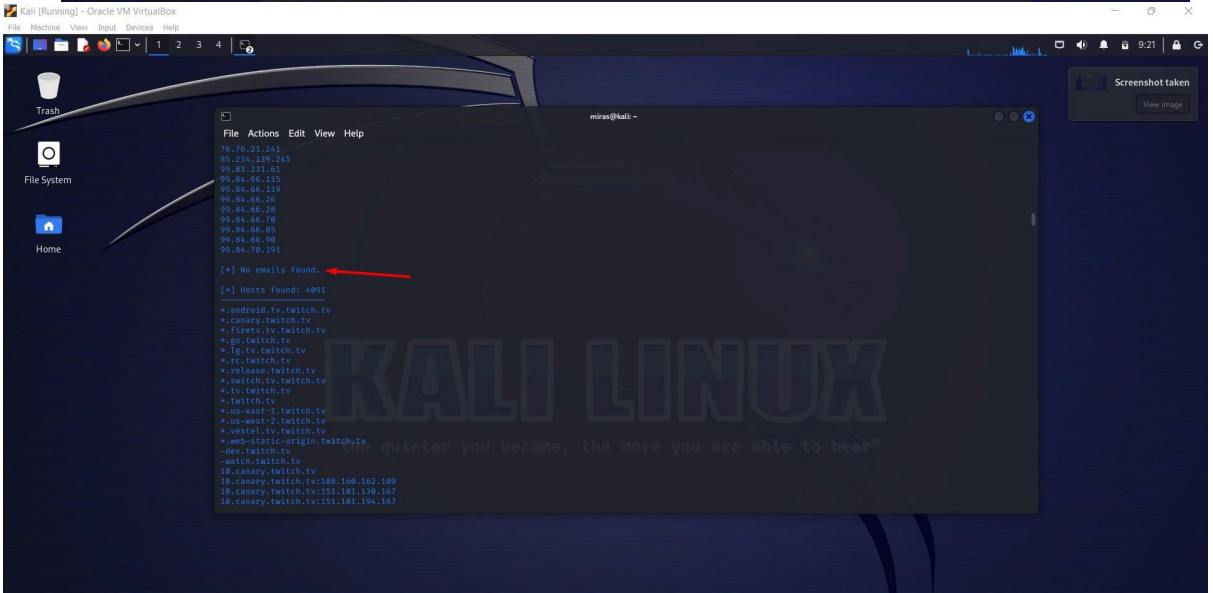






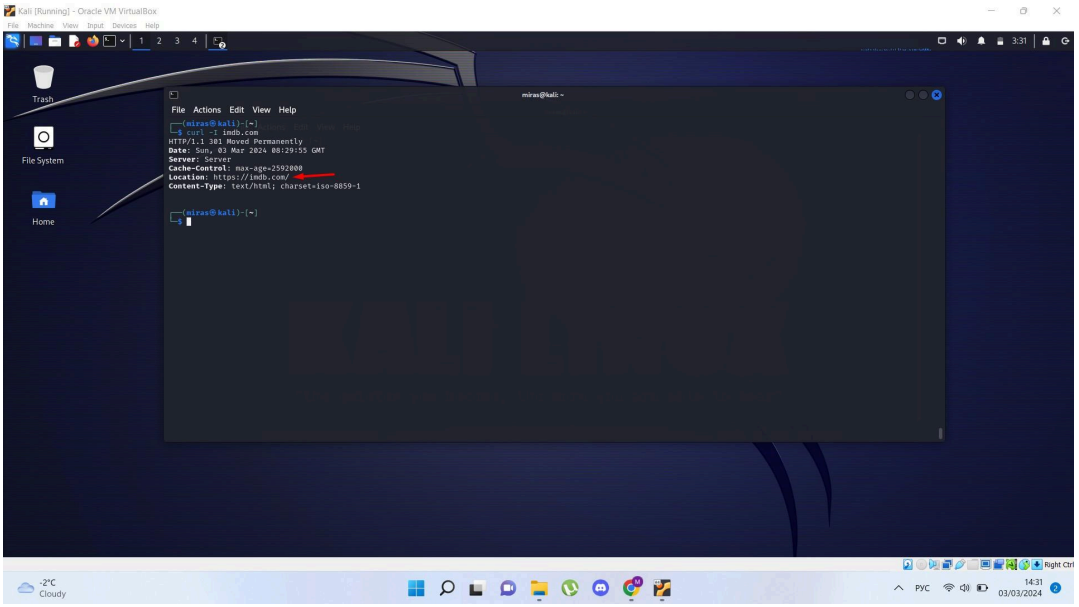

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
miras@kali: ~
File Actions Edit View Help
2606:4700:3037::681b:8414
2606:4700:30::681c:1074
2606:4700:30::681c:1174
2a06:98c1:3120::3
2a06:98c1:3120::c
2a06:98c1:3121::3
64.79.108.154
74.122.195.39
94.23.22.188
[*] No emails found.
[*] Hosts found: 19
*.vulnhub.com
blog.vulnhub.com:104.21.42.126
blog.vulnhub.com:172.67.162.8
blog.vulnhub.com:188.114.96.7
blog.vulnhub.com:188.114.97.7
blog.vulnhub.com:2606:4700:3030::6815:2a7e
blog.vulnhub.com:2606:4700:3030::ac43:a208
ctf-team.vulnhub.com
ctf-team.vulnhub.com:104.21.42.126
ctf-team.vulnhub.com:172.67.162.8
ctf-team.vulnhub.com:2606:4700:3030::6815:2a7e
ctf-team.vulnhub.com:2606:4700:3030::ac43:a208
download.vulnhub.com
download.vulnhub.com:104.21.42.126
download.vulnhub.com:172.67.162.8
download.vulnhub.com:2606:4700:3030::6815:2a7e
download.vulnhub.com:2606:4700:3030::ac43:a208
staging.vulnhub.com
staging.vulnhub.com:172.67.162.8
(miras㉿kali)-[~]
$
-5°C
Cloudy
ENG
US
20:47
03/03/2024

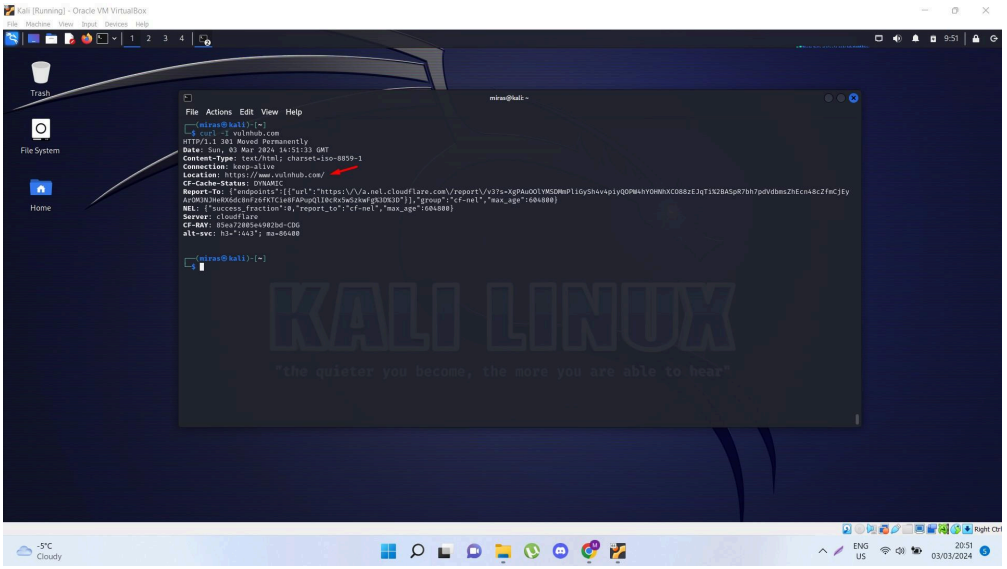

Kali [Running] - Oracle VM VirtualBox
Trash
File System
Home
miras@kali: ~
File Actions Edit View Help
Not valid before: Sep 1 21:33:12 2023 GMT
Not valid after: Oct 2 21:33:11 2024 GMT
(miras㉿kali)-[~]
(miras㉿kali)-[~]
$ theHarvester -d twitch.tv -b all
* theHarvester 4.4.4
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: twitch.tv
[!] Missing API key for bevigil.
[!] Missing API key for binaryedge.
[!] Missing API key for bufferoverun.
[!] Missing API key for Censys ID and/or Secret.

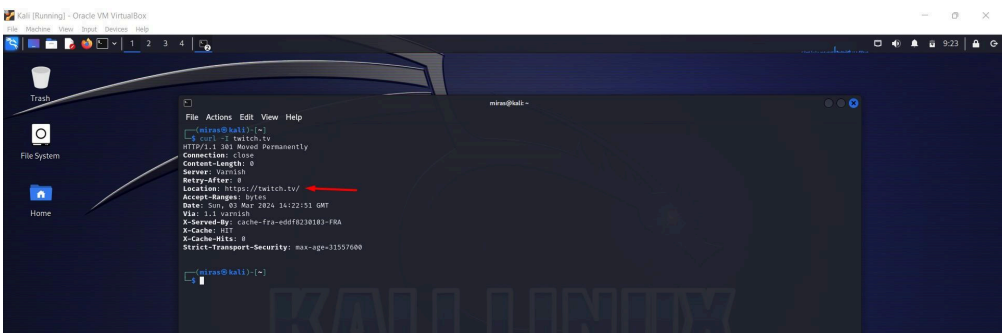

Kali [Running] - Oracle VM VirtualBox
Trash
File System
Home
Screenshot taken
View image
miras@kali: ~
File Actions Edit View Help
76.76.21.241
85.234.139.245
99.83.231.61
99.84.66.115
99.84.66.119
99.84.66.26
99.84.66.20
99.84.66.70
99.84.66.85
99.84.66.90
99.84.70.191
[*] No emails found.
[*] Hosts found: 4091
*.android.tv.twitch.tv
*.canary.twitch.tv
*.firetv.tv.twitch.tv
*.go.twitch.tv
*.lg.tv.twitch.tv
*.rc.twitch.tv
*.release.twitch.tv
*.switch.tv.twitch.tv
*.tv.twitch.tv
*.twitch.tv
*.us-east-1.twitch.tv
*.us-west-2.twitch.tv
*.vestel.tv.twitch.tv
*.web-static-origin.twitch.tv
-dev.twitch.tv
-watch.twitch.tv
10.canary.twitch.tv
10.canary.twitch.tv:108.160.162.109
10.canary.twitch.tv:151.101.130.167
10.canary.twitch.tv:151.101.194.167

15) Provide the HTTP headers used by domain or subdomains.

The curl -I command in Kali Linux fetches and displays only the HTTP headers from a specified URL.

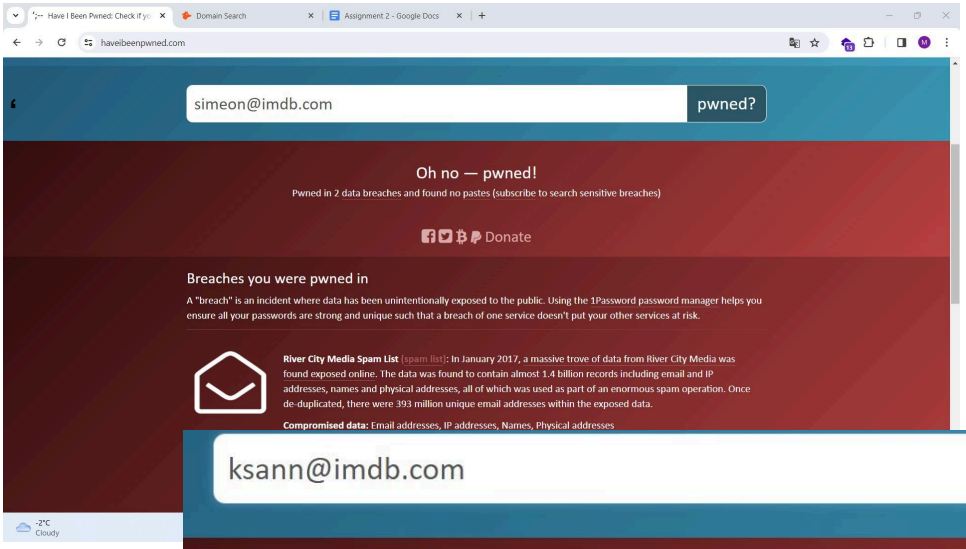


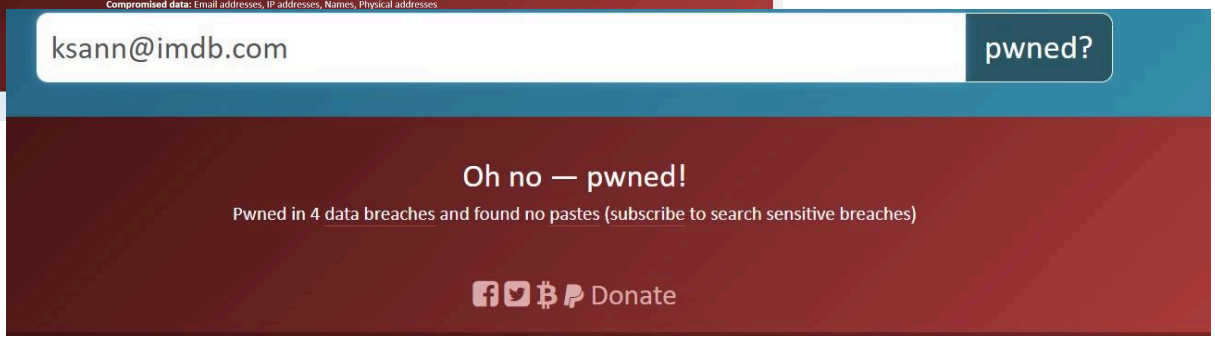


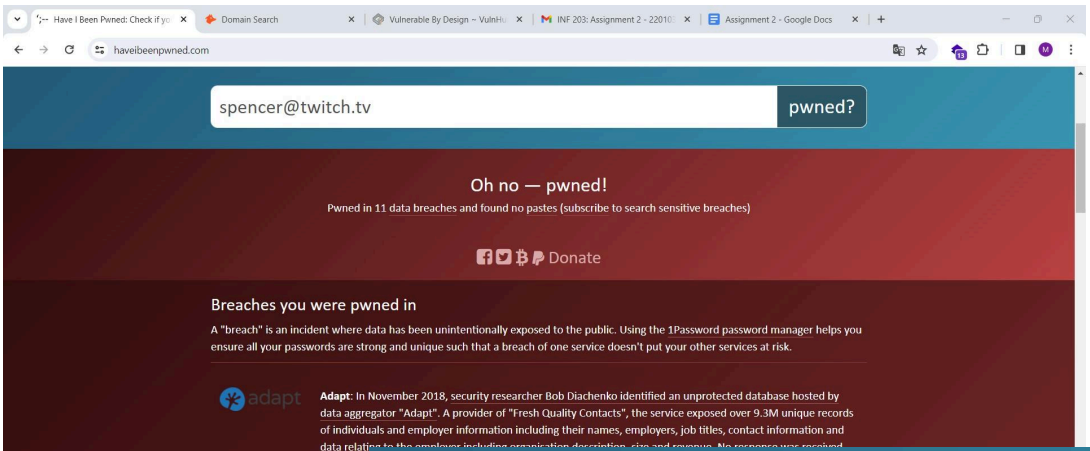


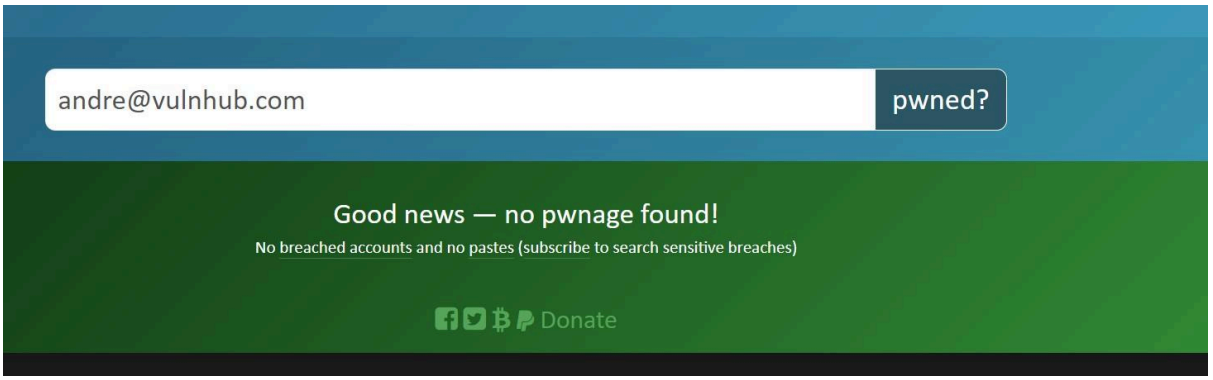
16) Provide a list of hacked email addresses of the organization.

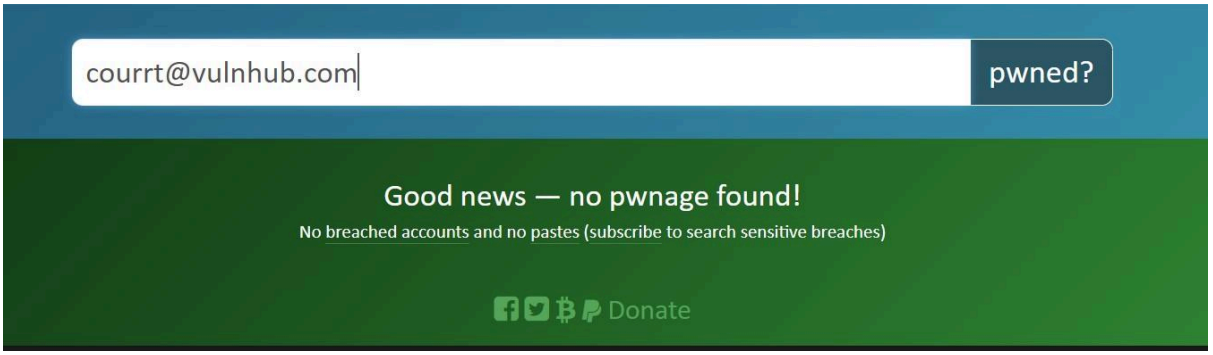
HaveIBeenPwned informs users whether their personal information has been compromised in data breaches.

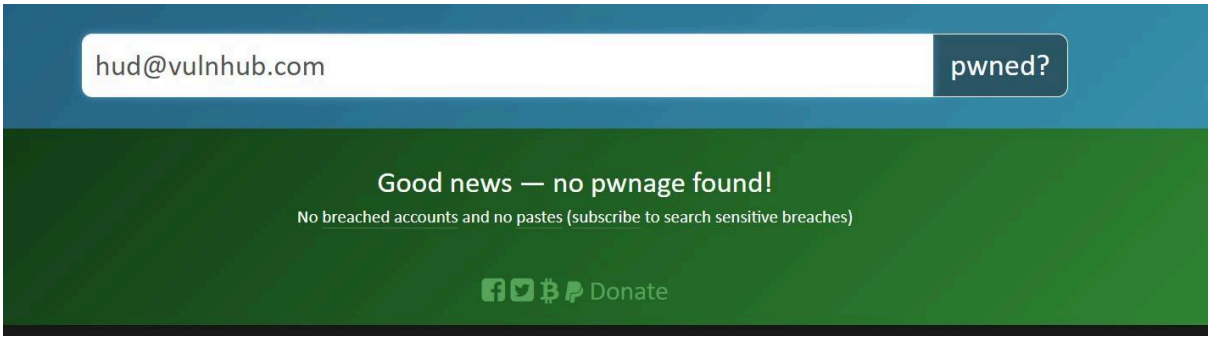







andre@vulnhub.com
pwned?
Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)
Donate


courrt@vulnhub.com
pwned?
Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)
Donate


hud@vulnhub.com
pwned?
Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)
Donate