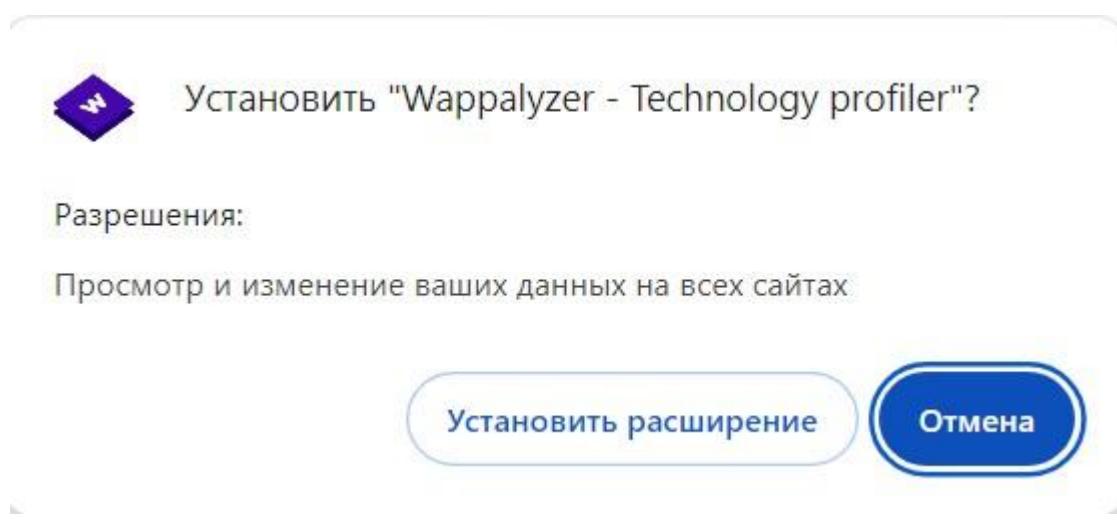


Berikov Miras
220103187

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](#)

A screenshot of a Microsoft Edge browser window displaying the IMDb homepage. The Wappalyzer extension is active, showing a sidebar with detected technologies. The sidebar includes sections for "TECHNOLOGIES", "MORE INFO", and "Export". Key technologies listed include: Электронная коммерция (Amazon Webstore), Аналитика (comScore), JS-фреймворк (styled-components, Next.js 12.3.4, React), Безопасность (HSTS), Веб-сервер (Next.js 12.3.4), Язык программирования (Node.js), CDN (Amazon CloudFront), Рекламная сеть (Amazon Advertising), and Утилита для разработчиков (styled-components). A "Featured today" banner for 'The Strangers: Chapter 1' is visible on the left.

A second screenshot of the Microsoft Edge browser on the same IMDb page, showing a different view of the Wappalyzer sidebar. This view shows technologies grouped under "Безопасность" (HSTS), "Веб-фреймворк" (Next.js 12.3.4), "Прочее" (Webpack 50% sure, Open-Graph, HTTP/2, Module Federation), "Утилита для разработчиков" (styled-components 6.1.0, Next.js 12.3.4, Swiper, Lodash 4.17.21, core-js 3.20.2, PaaS, Amazon Web Services), and "Генератор статических сайтов" (Next.js 12.3.4).

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

2 - vulnhub.com

The screenshot shows the Vulnhub website with a list of virtual machines. The sidebar on the right, titled 'Wappalyzer', lists various technologies used on the site, including:

- Аналитика**: Google Analytics (GA4)
- Прочее**: RSS, Open Graph, HTTP/3
- UI Фреймворк**: Bootstrap 4.4.1
- CDN**: jQuery CDN, Cloudflare
- JS-библиотека**: jQuery 3.4.1

Google Analytics - the most popular website analytics platform.

3 - twitch.tv

The screenshot shows the Twitch website with a list of recommended channels. The sidebar on the right, titled 'Wappalyzer', lists various technologies used on the site, including:

- Аналитика**: comScore, Google Analytics (GA4)
- Прочее**: Webpack, Open Graph, Module Federation
- Языки программирования**: TypeScript, GraphQL
- Безопасность**: Kasada, HSTS
- Рекламная сеть**: Amazon Advertising
- Шрифт**: Font Awesome

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

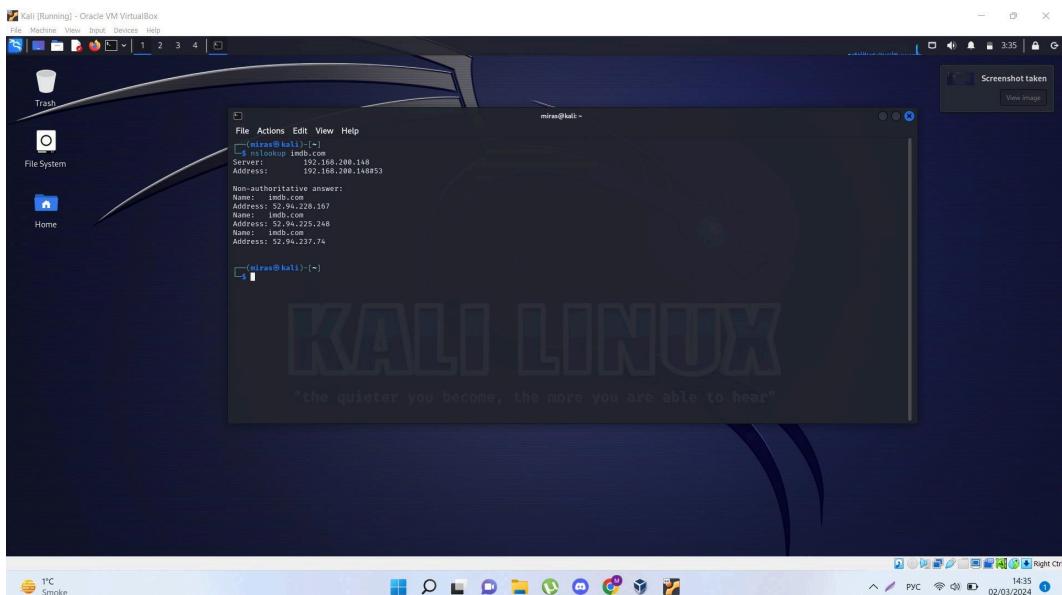
UI Framework: Bootstrap; **JS-library:** jQuery; **CDN:** jQuery CDN, Cloudflare

3 - twitch.tv

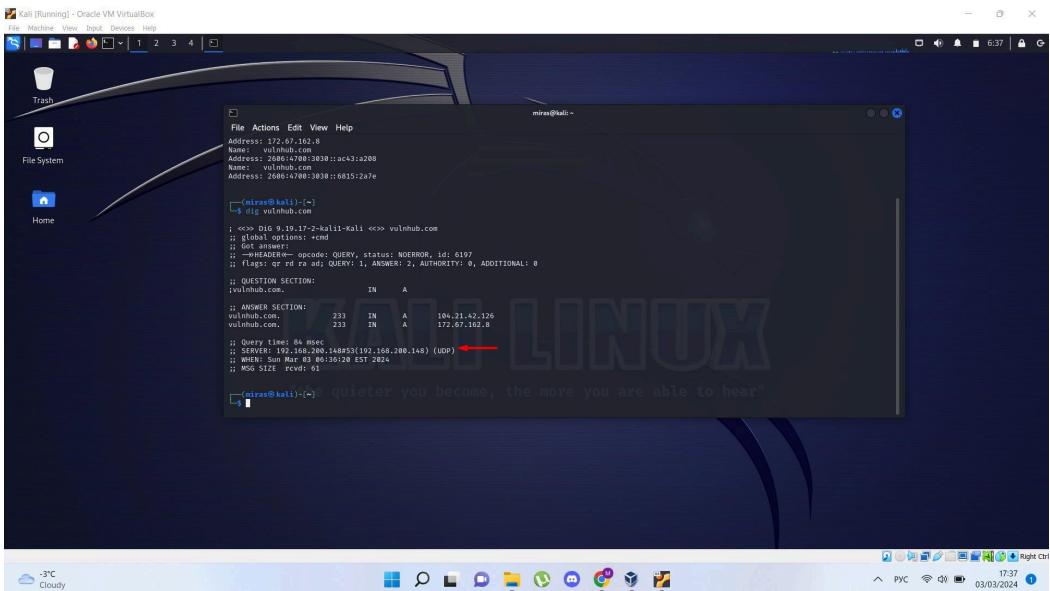
JS-framework: styled-components, React, Vue.js; **Programming Language:** TypeScript, GraphQL; **Security:** Kasada, HSTS, **JS Library:** core-js, Apollo

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

1 - imdb.com

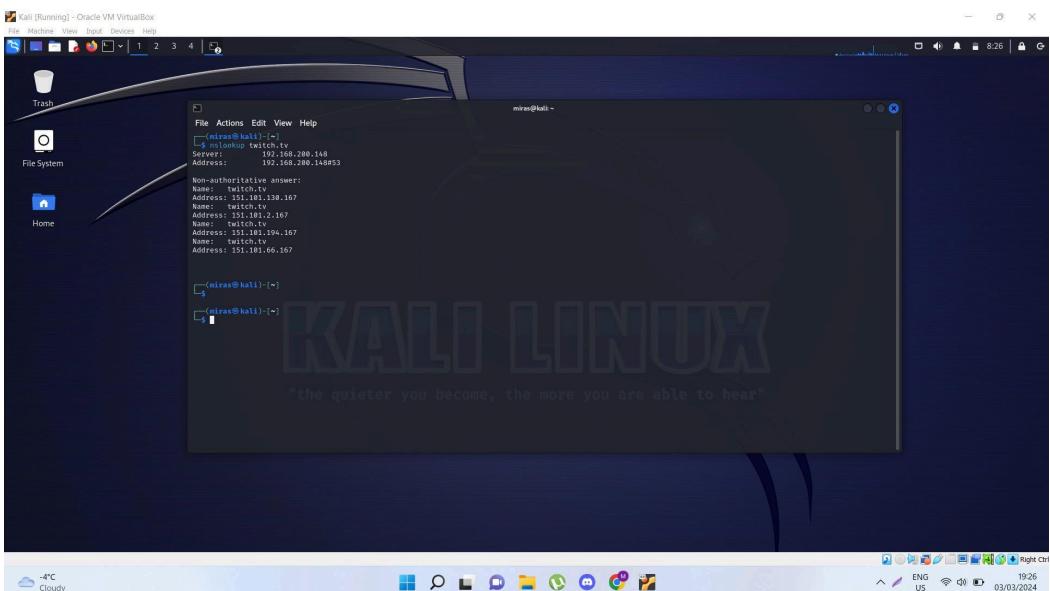


2 - vulnhub.com



```
mira@kali:~$ dig vulnhub.com
; <>> SIG 9:19.17-2=kali-Kali <>> vulnhub.com
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; Got answer:
;; HEADER=rrc opcode: QUERY, status: NOERROR, id: 6197
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;vulnhub.com.           IN  A
;; ANSWER SECTION:
vulnhub.com.        233   IN  A   104.21.42.126
;; Query time: 86 msec
;; TTL: 1440000000 (200.14853192.169.280.148) (UDP)
;; WHEN: Sun Mar 03 05:36:12 EST 2024
;; MSG SIZE rcvd: 61
mira@kali:~$ quieter you become, the more you are able to hear"
```

3 - twitch.tv

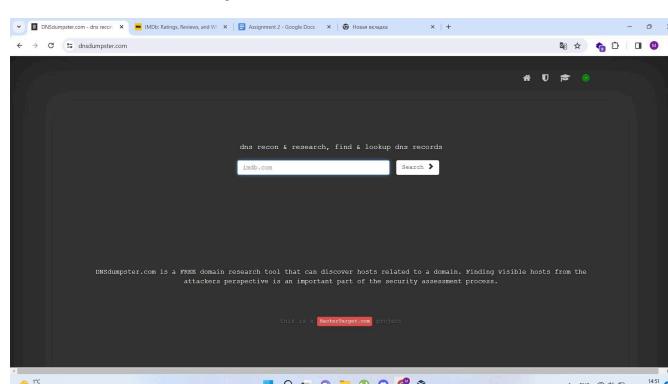


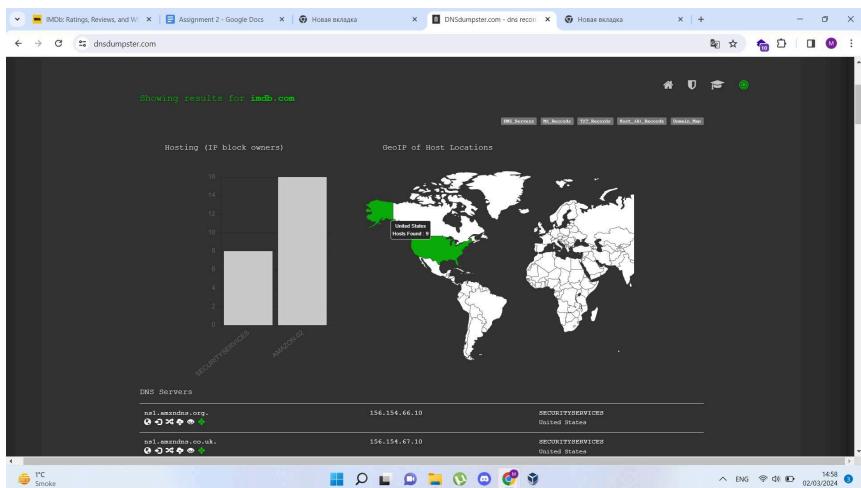
```
mira@kali:~$ nslookup twitch.tv
Server: 192.168.200.148
Address: 192.168.200.148#53
Non-authoritative answer:
Name: twitch.tv
Address: 151.101.108.167
Name: twitch.tv
Address: 151.101.2.167
Name: twitch.tv
Address: 151.101.109.167
Name: twitch.tv
Address: 151.101.66.167
mira@kali:~$ 
mira@kali:~$
```

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.

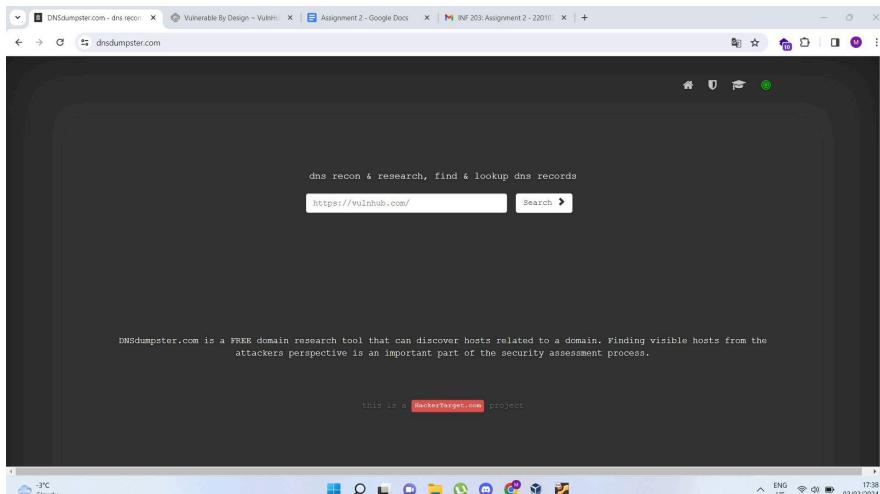
1 - imdb.com

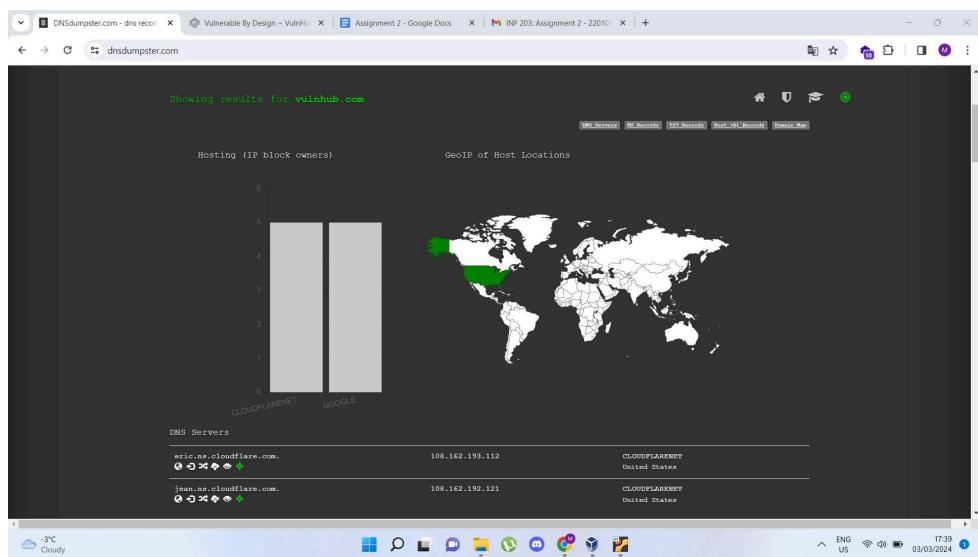




Host Records (A) <small>(this data may not be current as it uses a static database (updated monthly))</small>		
<code>origin-www-us2.imdb.com</code>	52.119.171.76	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>app.dd.imdb.com</code>	52.94.225.250	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>us.dd.imdb.com</code>	52.94.228.167	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>webservice.imdb.com</code>	52.94.228.186	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>secure.imdb.com</code>	52.94.227.74	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>contribute.imdb.com</code>	52.94.228.191	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>graphql1.imdb.com</code>	108.128.106.47 server-108-128-106-47.jfk50.r.cloudfront.net	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>dev.graphql1.imdb.com</code>	108.128.246.59 server-108-128-246-59.sfo5.r.cloudfront.net	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>opf-m.imdb.com</code>	52.94.225.254	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>origin-m.imdb.com</code>	52.94.225.254	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>origin-pro.imdb.com</code>	52.94.228.166	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>origin-help.imdb.com</code>	52.94.225.171	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>developer.imdb.com</code>	18.160.10.9 server-18-160-10-9.iad12.r.cloudfront.net	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>origin-www.imdb.com</code>	52.94.225.248	AMAZON-02 United States
HTTP: <code>Server</code>		
<code>apx-security.imdb.com</code>	52.46.149.74	AMAZON-02 United States
HTTP: <code>Server</code>		

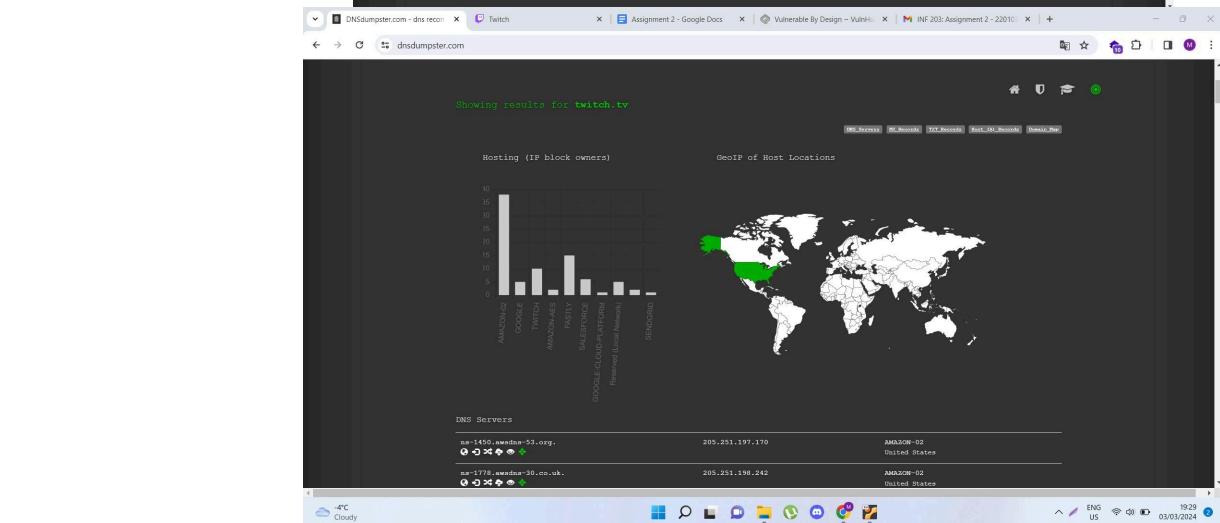
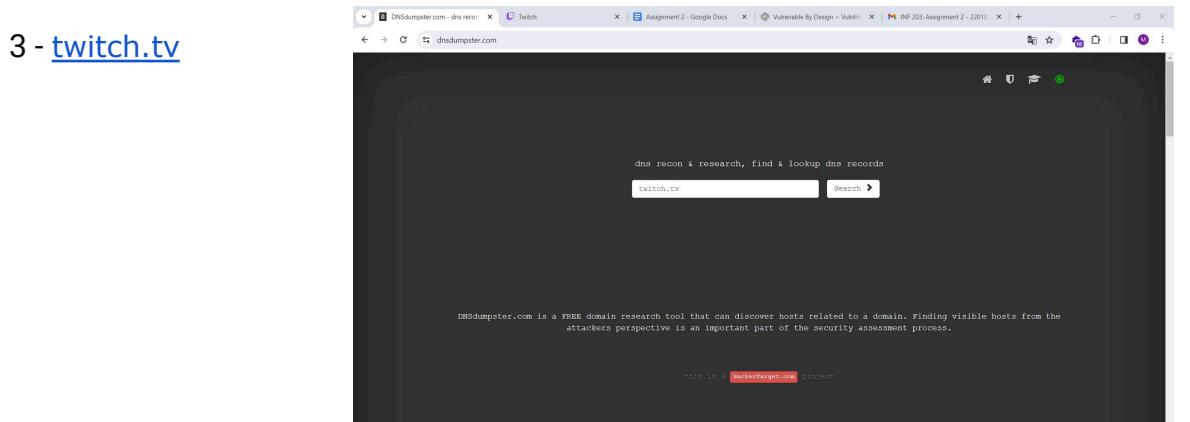
2 - vulnhub.com





Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
download.vulnhub.com	172.67.162.8	CLOUDFLARENFT United States
staging.vulnhub.com	172.67.162.8	CLOUDFLARENFT United States
www.vulnhub.com	104.21.42.126	CLOUDFLARENFT unknown

3 - [twitch.tv](#)





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

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

1 - [imdb.com](https://www.linkedin.com/company/imdb-com/)

The screenshot shows the LinkedIn company profile for IMDb.com. It displays a banner for 'IMDb Join the cast' and information about the company being an Entertainment Providers based in Seattle, Washington, with 133,902 followers. A red arrow points to the 'View all 1,020 employees' link. To the right, there's a section for 'Affiliated pages' listing 'Amazon Software Development Seattle, WA'. Below that is a section for 'Similar pages' listing 'Netflix Entertainment Providers Los Gatos, CA', 'Focus Features Entertainment Providers', 'Letterboxd Entertainment Providers Auckland, AKL', and 'Prime Video & Amazon Studios Entertainment Providers Seattle, Washington'. There are also sections for 'About us', 'Browse jobs', and a footer with system icons.

The screenshot shows LinkedIn search results for people at IMDb.com. It displays a list of 1,000 results, each showing a profile picture, name, title, and current location. On the right side, there's a promotional image for LinkedIn's hiring feature. The interface includes standard LinkedIn navigation bars like Home, My Network, Jobs, Messaging, Notifications, and Me.

The screenshot shows the Hunter.io Email Finder tool. It has a search bar where 'Kelvin Chan' is entered, followed by '@imdb.com' and a 'Find' button. Below the search bar, it shows a contact card for Kelvin Chan with a yellow KC icon, an acceptance rate of 78%, and a note that the email is accept-all. It also says 'We didn't find this email address publicly on the web.' To the right, a summary box states 'We found 112 email addresses for imdb.com' and 'Find the list of email addresses associated with this company that are publicly available on the web.' There are 'See all results' and 'Email Finder' buttons. The bottom of the screen shows the Windows taskbar with various open tabs and system icons.

imdb.com

Type Department Show only results with

112 results for your search Export Find by name

Katie Sann +1 206 922 0636
ksann@imdb.com Interactive Media Save as lead Add to a campaign

94%
20+ sources

Greg Bulmash +1 206 922 0636
greg@imdb.com Interactive Media Save as lead Add to a campaign

94%
20+ sources

Jon Reeves Executive Producer
jreeves@imdb.com Save as lead Add to a campaign

94%
20+ sources

Emily Glassman +1 206 266 8077
Emily.Glassman@imdb.com Event Producer

2 - [vulnhub.com](#)

vulnhub.com

Люди Контакты Регионы Текущая компания Все фильтры

125 результатов

Участник LinkedIn
Junior Threat Detection Analyst at Alchemy Security, LLC
Greater Colorado Springs Area
Проекты: Self study hacking with VulnHub - ...[vulnhub.com](#) running on a host only network inside...

Участник LinkedIn
Network security engineer | ITI graduate -Cyber security associate | Palotto [...] Cairo, Egypt
Проекты: OSCP-Like CTF-Challanges : walk-through for boot2root VM from [VulnHub.com](#) (easy)

Участник LinkedIn
IT Service Delivery Manager | Project & Program Management Professional [...] Dubai, United Arab Emirates
Публикации: Vulnhub : VulnOS : 2 Walkthrough - This is my write-up for VulnOS:2 at [Vulnhub.com](#). About [vulnhub.com](#) Vulnhub is a community driven...

Участник LinkedIn
Cyber Security Engineer | CTF player | Ethical hacker | VAPT | Bug hunter... Bengaluru
Current: Machine hacking – [Vulnhub.com](#)

Участник LinkedIn
A Cyber-Security Professional, Enthusiastic & Learner | Making Industries... Delhi, India
Официальные соревнования challenges available on "HackTheBox.com" and "[VulnHub.com](#)" | Have A

Screenshot of a web browser showing multiple tabs open, including "Email Finder", "Vulnerable By Design - Vulnhub", "Assignment 2 - Google Docs", and "INF 203: Assignment 2 - 2010". The "Email Finder" tab displays search results for "Hud Daanna" and "Sameh Ammar".

Email Finder

Hud Daanna @ vulnhub.com Find

Hud Daanna hud@vulnhub.com Save as lead Add to a campaign

We didn't find this email address publicly on the web.

Sameh Ammar

sameh@vulnhub.com Save as lead Add to a campaign

75% This email is accept-all. Learn more

We didn't find this email address publicly on the web.

3 - [twitch.tv](#)

Screenshot of the LinkedIn search results for "twitch.tv". The search bar shows "twitch.tv". The results list several LinkedIn profiles of Twitch streamers.

LinkedIn Header: twitch.tv Главная Сеть Вакансии Сообщения Уведомления Профиль Для бизнеса Попробовать Premium за 0 USD

Люди | Контакты | Регионы | Текущая компания | Все фильтры

Подробнее о 23 000 результатах

 Участник LinkedIn Influencer & Streamer at Twitch Istanbul, Turkey Current: Streamer – Twitch	 See who's hiring on LinkedIn. 
 Участник LinkedIn DS at Twitch.tv San Francisco Bay Area Current: Director, Data Science – Twitch	
 Участник LinkedIn Streamer Host @ twitch.tv/eddieoztv Tallinn Current: Streamer @ twitch.tv/eddieoztv – EddieOzTV	
 Участник LinkedIn Founder, President & CEO of DRIVE ENTERTAINMENT GROUP: TV & FILM... New York, NY Current: DJ/CONTENT CREATOR on TWITCH (DJAVIVA) – Twitch	
 Участник LinkedIn Information Technology Coordinator twitch.tv/Vartan13 Istanbul Current: Twitch.tv/Vartan13 – Twitch	

Twitch

Domain Search

twitch.tv

159 results

Spencer Nelson
spencer@twitch.tv
94%
20+ sources

Cody Wohlers
codywohlers@twitch.tv
94%
1 source

Matthew Dipietro
matt@twitch.tv
94%
7 sources

Company

Twitch
Twitch is an interactive live streaming service for content spanning gaming, entertainment, sports, music, and more. There's som... more

Email pattern: {first}{last}@twitch.tv
Accept all: YES
Industry: Software Development
Headcount: 1001-5000
Address: San Francisco, California, United States

Technologies

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)

site:imdb.com credentials

FIGHT]] Jake Paul vs Ryan Bourland LIVE Free 2024

FIGHT] Jake Paul vs Bourland LIVE TV Coverage 2024

FIGHT-LIVE] Jake Paul vs Ryan Bourland LIVE Coverage

In order to show you the most relevant results, we have omitted some entries very similar to the 265 already displayed.
If you like, you can repeat the search with the omitted results included.

Kazakhstan Almaty - From your IP address - Update location

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

The screenshot shows a Google search results page with the query "site:vulnhub.com Credentials". The results list several vulnhub.com entries, each with a thumbnail icon, the site name, a URL, and a brief description. A red arrow points to the top of the scroll bar on the right side of the window.

- Bot Challenges**
The objective of this vulnerable virtual machine is to get a root shell. The root **credentials** (for network configuration purposes) are root:password. These ...
- Frequently Asked Questions**
Q.) What are the dangers/security issues of running an (unknown) virtual machine? Q.) What can I do to protect my network and myself? Q.) VMware is telling me: ...
- Metasploitable: 1**
A number of vulnerable packages are included, including an install of tomcat 5.5 (with weak **credentials**), distcc, tikiwiki, twiki, and an older mysql. You ...
- WebGOAT**
Sep 16, 2019 — **Credentials**: - user: webgoat - pass: webgoat. This machine is used to practice on different types of web attacks. Enjoy! more... WebGOAT: 1.
- Tommy Boy**
Jul 27, 2016 — ... **credentials** is Tom Callahan Sr. - who just passed away! And to make matters worse, the only other guy with knowledge of the server just quit ...
- Secarmy Village**
In case the IP doesn't show up you can log into the machine using our test account **credentials**: cero:svos. GOODLUCK! more... Secarmy Village: Grayhat ...

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

The screenshot shows a Google search results page with the query "site:twitch.tv Credentials". The results list several twitch.tv entries, each with a thumbnail icon, the site name, a URL, and a brief description. A red arrow points to the top of the scroll bar on the right side of the window.

- Getting OAuth Access Tokens**
Client **credentials** grant flow, App access token, Use this flow if your app uses a server, can securely store a client secret, and can make server-to-server ...
- Unable to Retrieve OAuth Client **Credentials** Token (Invalid ...**

Mar 1, 2022 — I'm trying to develop an application that can get notifications when someone follows or subscribes to a channel. However, I cannot seem to ...

- Getting OAuth **credentials** in an app without a server - API**
Mar 22, 2023 — Getting OAuth **credentials** in an app without a server ... Hi, I'm looking into making a UES plugin to perform twitch integration. I believe that ...

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

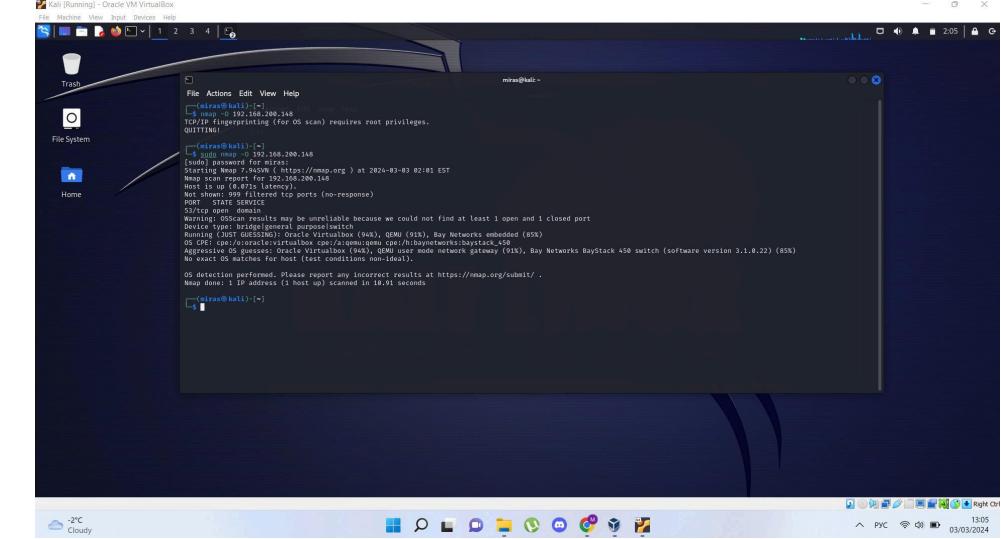


Din webbläsare kan inte spela upp den här videon. AWS. The Safe Room: Responding to Security Events | EP1 | Protecting AWS IAM **credentials**. 46 ...
Twitch · Dec 14, 2021

*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



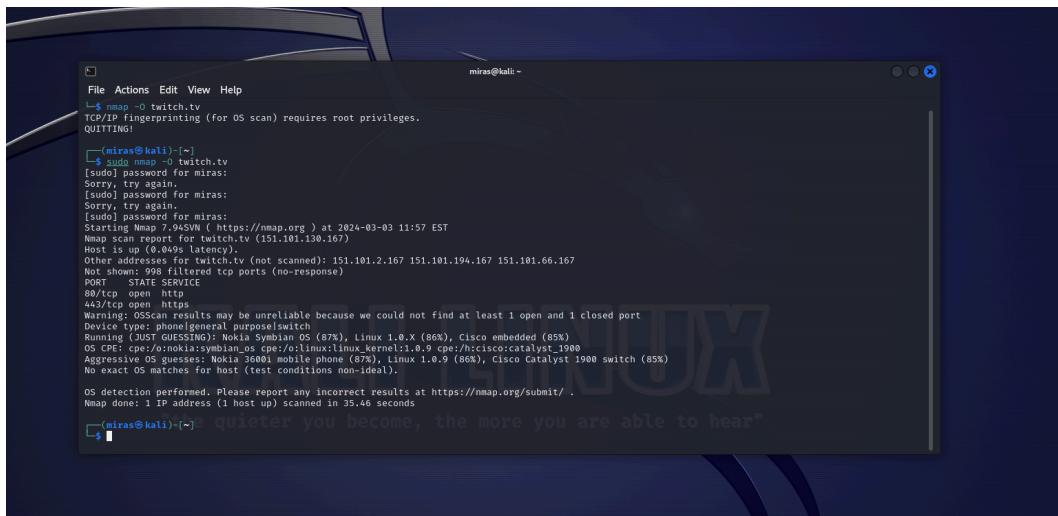
```
mirs@kali:~$ nmap -O 192.168.200.148
[sudo] password for mirs:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-03 02:03 EST
Nmap scan report for 192.168.200.148
Host is up (0.075s latency).
Other addresses for 192.168.200.148 (not scanned): 172.0.1.102
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge/general purpose switch
Running: QNAP (95%), Oracle VM VirtualBox (4%), Bay Networks embedded (0%)
```

2 - vulnhub.com



```
mirs@kali:~$ nmap -O 192.168.21.126
[sudo] password for mirs:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-03 07:13 EST
Nmap scan report for 192.168.21.126
Host is up (0.075s latency).
Other address for 192.168.21.126 (not scanned): 172.0.1.102
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8000/tcp  open  http-proxy
8080/tcp  open  https-alt
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge/general purpose switch
Running: QNAP (95%), Oracle VM VirtualBox (4%), Bay Networks embedded (0%)
```

3 - twitch.tv



```
[miras@kali:~] nmap -O twitch.tv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 11:57 EST
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
[miras@kali:~] [sudo] password for miras:
Sorry, try again.
[sudo] password for miras:
Sorry, try again.
[sudo] password for miras:
Sorry, try again.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 11:57 EST
Nmap scan report for twitch.tv (151.101.130.167)
Host is up (0.049s latency).
Other addresses on host twitch.tv (not scanned): 151.101.2.167 151.101.194.167 151.101.66.167
Not shown: 999 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 35.46 seconds
[miras@kali:~] quieter you become, the more you are able to hear"
```

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

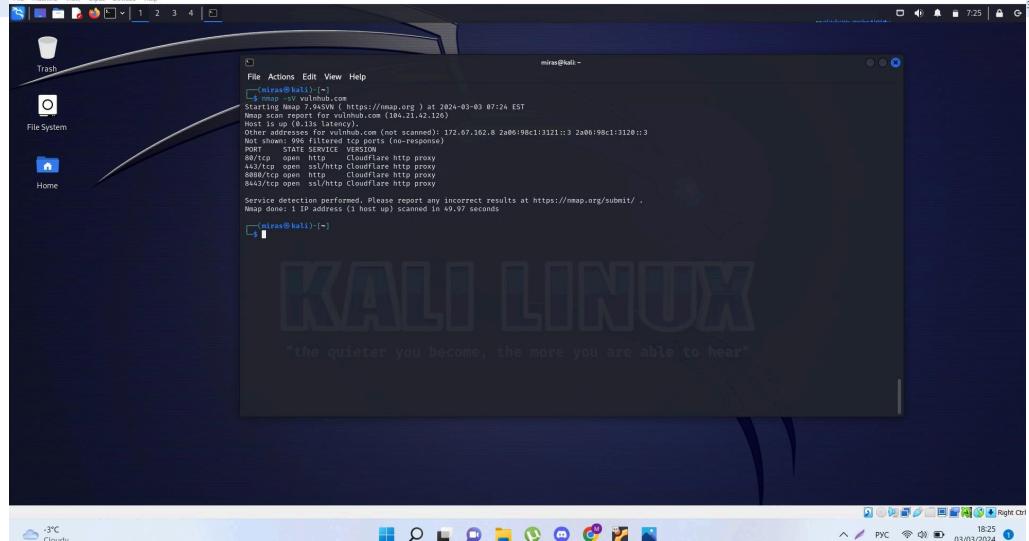
1 - imdb.com



```
[miras@kali:~] nmap -O imdb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 02:08 EST
Nmap scan report for imdb.com (52.94.237.74)
Host is up (0.24s latency).
Other addresses on host imdb.com (not scanned): 52.94.225.248 52.94.228.167
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http      Server
443/tcp   open  ssl/http  Server
2 services unversioned despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service

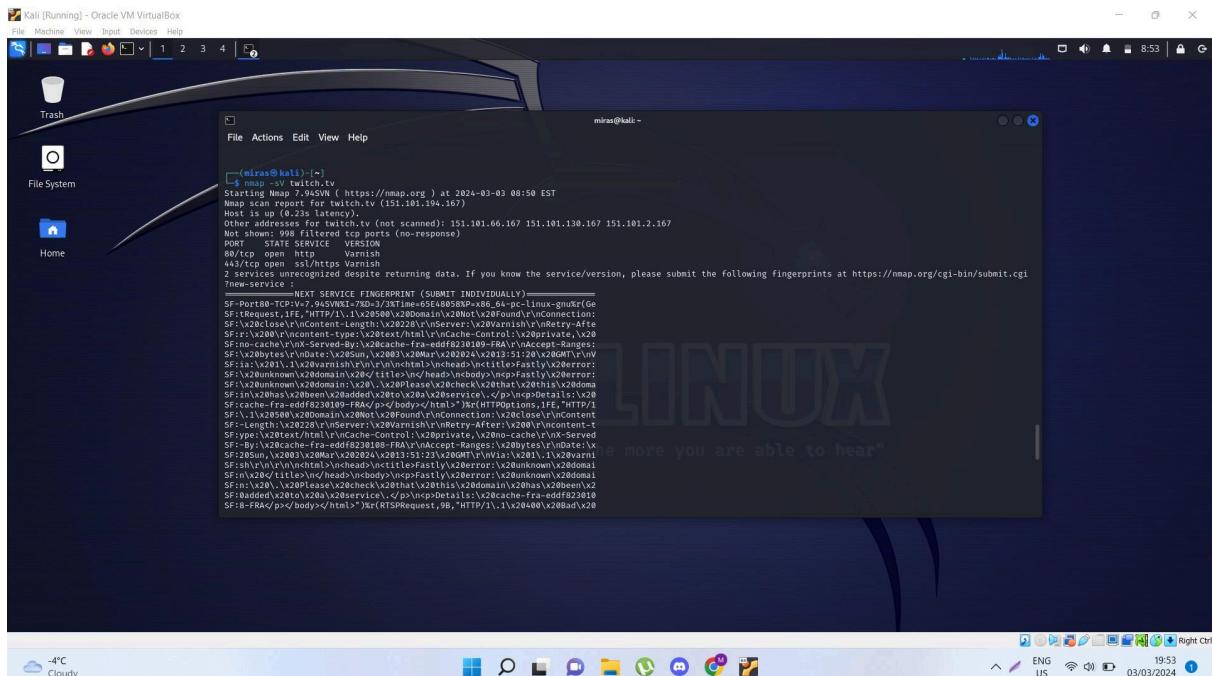
[miras@kali:~] [miras@kali:~] [miras@kali:~]
```

2 - vulnhub.com



```
[miras@kali:~] nmap -O vulnhub.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 07:24 EST
Nmap scan report for vulnhub.com (104.21.42.126)
Host is up (0.11s latency).
Other addresses on host vulnhub.com (not scanned): 172.67.102.8 za06:98c1:3121::3 za06:98c1:3120::3
PORT      STATE SERVICE VERSION
80/tcp    open  http      Cloudflare http proxy
443/tcp   open  ssl/http Cloudflare http proxy
8080/tcp  open  http      Cloudflare http proxy
8443/tcp  open  ssl/http Cloudflare http proxy
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.97 seconds
[miras@kali:~] [miras@kali:~]
```

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)

DNS Servers			
ns1.amzndns.org.	156.154.66.10	SECURITYSERVICES	United States
ns1.amzndns.co.uk.	156.154.67.10	SECURITYSERVICES	United States
ns2.amzndns.net.	156.154.69.10	SECURITYSERVICES	United States
ns1.amzndns.net.	156.154.65.10	SECURITYSERVICES	United States
ns2.amzndns.co.uk.	204.74.120.1	SECURITYSERVICES	United States
ns2.amzndns.org.	156.154.150.1	SECURITYSERVICES	United States
ns1.amzndns.com.	156.154.64.10	SECURITYSERVICES	United States
ns2.amzndns.com.	156.154.68.10	SECURITYSERVICES	United States

MX Records ** This is where email for the domain goes...			
10 amazon-smtp.amazon.com.	44.231.24.41	AMAZON-02	United States
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations			
"IPROTA_D66964-XXX"			
"atlassian-domain-verification=ZT4AapXgobCpXIWoNcd7gtMjZyOudr4EDFMnFUWrgggdaQVbDvoGpRaIwj/tgPH"			
"adobe-idp-site-verification=b6bcd3e5affc63607c8bf75744d9a0d1febc50dd7f389428e2ae476c9ba8814"			
"v=spf1 include:amazon.com -all"			
"MS-ms74462343"			
"cisco-ci-domain-verification=5b0cade9b99903b93ec19495d546a72dbb24ecf17c3670b02bbf706bb9ba552a"			
"google-site-verification=f3PqOeHGPuPaaRkAPJ4bSO-08bDQoohrmwdxtJAIIM"			
"google-site-verification=uL7Y3ZHGF5c6a05oXtn2S2Vq6LfrtqsYlwzsK0yl8"			

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_asmdNg2CX0lhhPmssZm_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

```

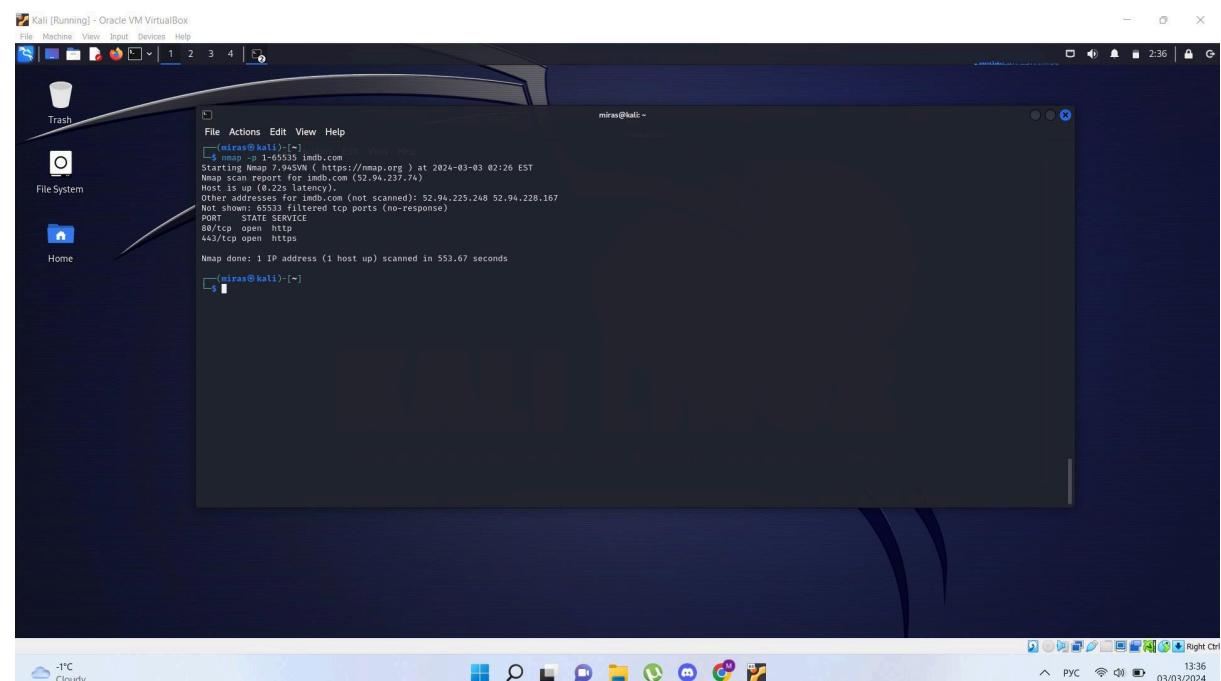
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"03vnqw0f74w2ssqpg6vtdpybnnk7v81k"
"MS=ms2992082"
"_globalsign-domain-verification=9Uioyer00_F2Epyd3gGV5_Vk1XzoibTukD_jkbZPe43"
"_globalsign-domain-verification=PeBo1xAMkWVF0qJ28xB-APP6cLPZNf6oB7m4jy94oR"
"amazonoses:103ntJItAHAS8zF3zrpl+RajxRQJ4t1PSC9BB4StgBk="
"amazonoses:36386uCaP/zadqoJqgFiBovDfvnRnQaIdSiMN2ck7I="
"amazonoses:E0blpTRNogJgo+NEwz1pCdbiA0W8uziSRCezsgdhTZ8="
"amazonoses:TS/Q8uPSq0t+/WbYLNgVUDzb1QD3Eg1T1FBxmkfz8kI="
"amazonoses:cpm2Dn+xS6T56Iq1KBjzLE3E7OsD2vAoCQIyxvcVgplc="
"amazonoses:lZzYXC4khwzoy6SooezLVTpF8e7/Jh3JMUYqv0bWI="
"amazonoses:n0xA4rjoeQ1tK6vzeRBViDtPhuXpqsnntVALqWAfEz0="
"amazonoses:q1VqNqptpdPoDMi8EixEYsLNRMPlp5xGIY3uOpUdDHQ="
"amazonoses:wzbVR0BrJcHgXdo623myecXiqm4USLX3kIgSKymaVso="
"atlassian-domain-verification=PR1WNTa0H2F2sDQVhpCAAxSgaKScDpfZdE1Df4abvU1/BTE2BMDRNWCxxHYAWFRa"
"bugcrowd-verification=4cb1e80d1cc53286a15726ee4bf8f6e"
"cisco-ci-domain-verification=132cb07ebad7bdalf2d4659730b12d115c80a95b6c4e5303a010f3edef248906"
"docusign=79f74da0-0f98-4cdb-b2d3-93871ea127c8"
"google-site-verification=9rDIUbekFpQoTOIBeCYKmEbmngrR6Dp9nJ72qLBBwOE"
"google-site-verification=hDc28WSCJ_PZVKa2N60VvD2UqCbxUX81mmBP8QJn0"
"google-site-verification=xYplJj114xfWi8VIM2NFMQUeIbrKUg9achbQ5W4AYJA"
"sending_domain1020022=834b5b18e26655468c764e5279df6460ed66057be1d8c0684722b8c589b35add"
"spring-site-verification=p7Ka5X9lnBvzD3p1B6lcrXfhabY2uX3NawyEGPm4C98"
"stripe-verification=98fd69ef9979b0dcdc41fc6ea416633b9cd2e008a989b1c64732897a272bb804"
"twilio-domain-verification=7471ef203449152cf7ec9a3d518a82"
"uber-domain-verification=18c3e151-508f-477d-87fb-23e876237df1"
"v=spf1 include:_spf.google.com include:amazonoses.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.



2

```
(miras@kali)-[~]
$ nmap -p- -T4 vulnhub.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 10:06 EST
Stats: 1:03:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 32.82% done; ETC: 13:19 (2:09:59 remaining)
```

3

```
(miras@kali)-[~]
$ nmap -p- -T4 twitch.tv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 10:07 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 18.05 seconds

(miras@kali)-[~]
$ nmap -p- -T4 twitch.tv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 10:09 EST
Nmap scan report for twitch.tv (151.101.2.167)
Host is up (0.27s latency).
Other addresses for twitch.tv (not scanned): 151.101.66.167 151.101.130.167 151.101.194.167
Not shown: 65533 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 6401.72 seconds

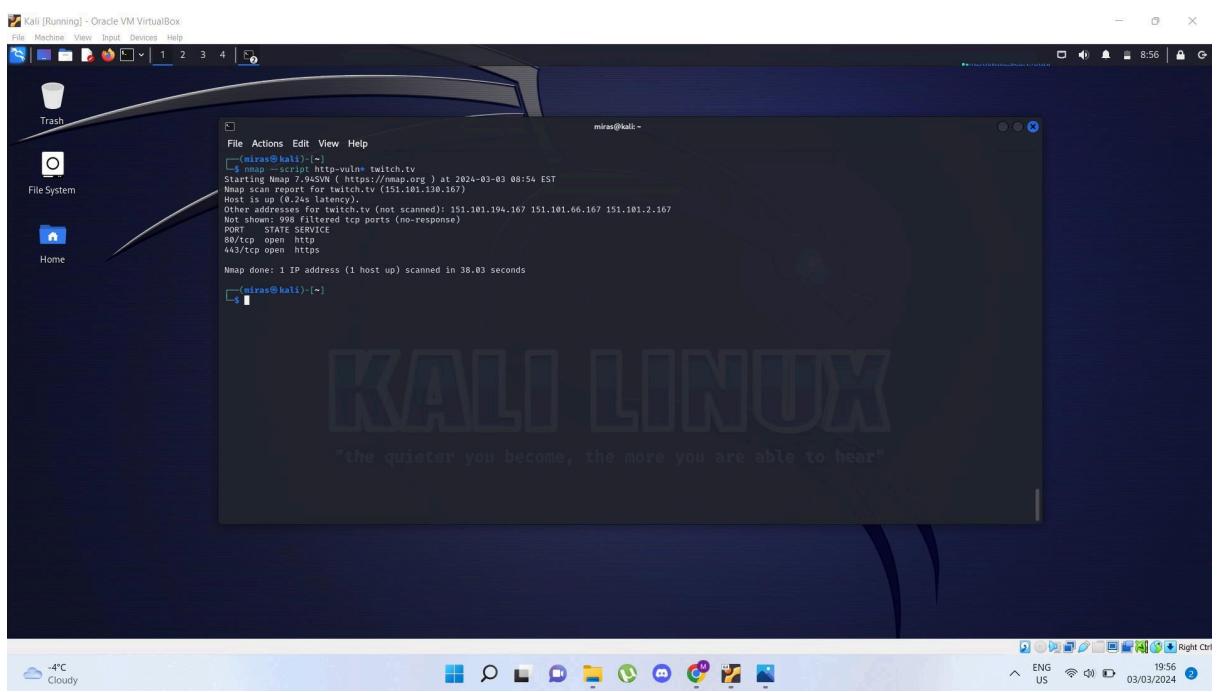
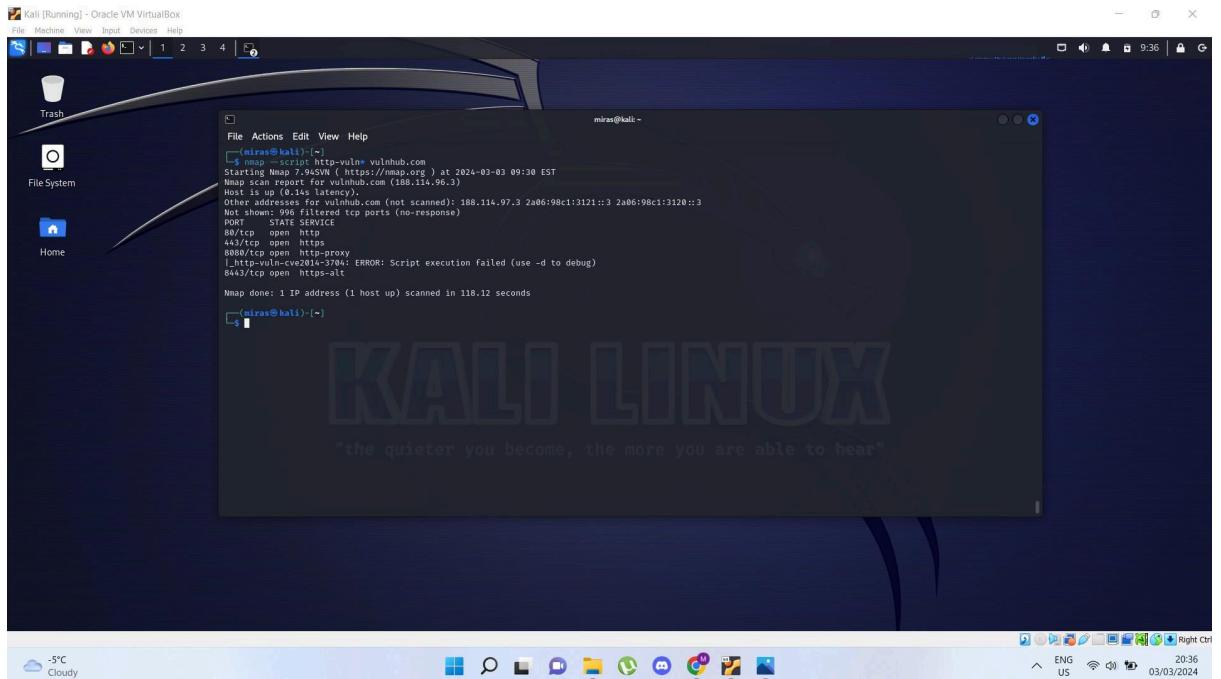
(miras@kali)-[~]
```

12) Find possible vulnerabilities related to HTTP using NSE.

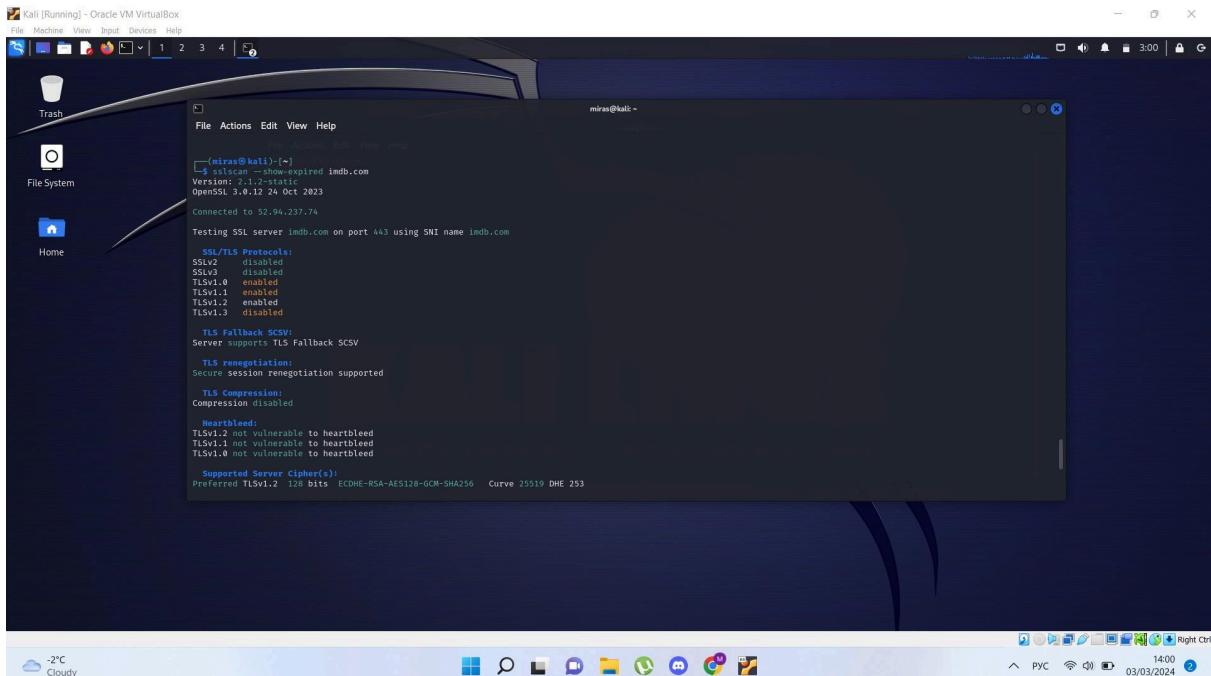
```
(miras@kali)-[~]
$ nmap --script http-vuln* imbd.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 02:42 EST
Nmap scan report for imbd.com (92.94.225.248)
Host is up (0.23s latency).
Other addresses for imbd.com (not scanned): 52.94.228.167 52.94.237.74
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 33.02 seconds

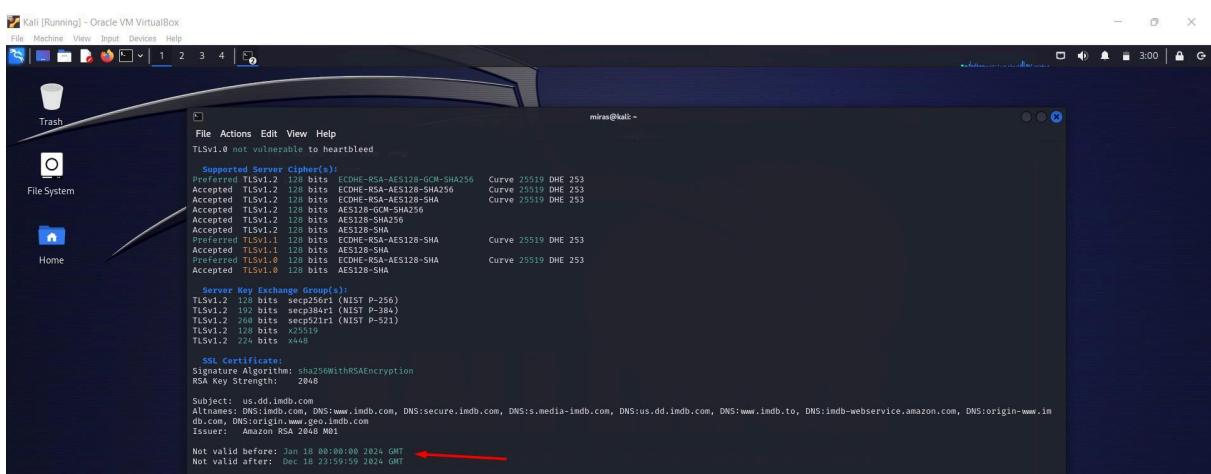
(miras@kali)-[~]
```



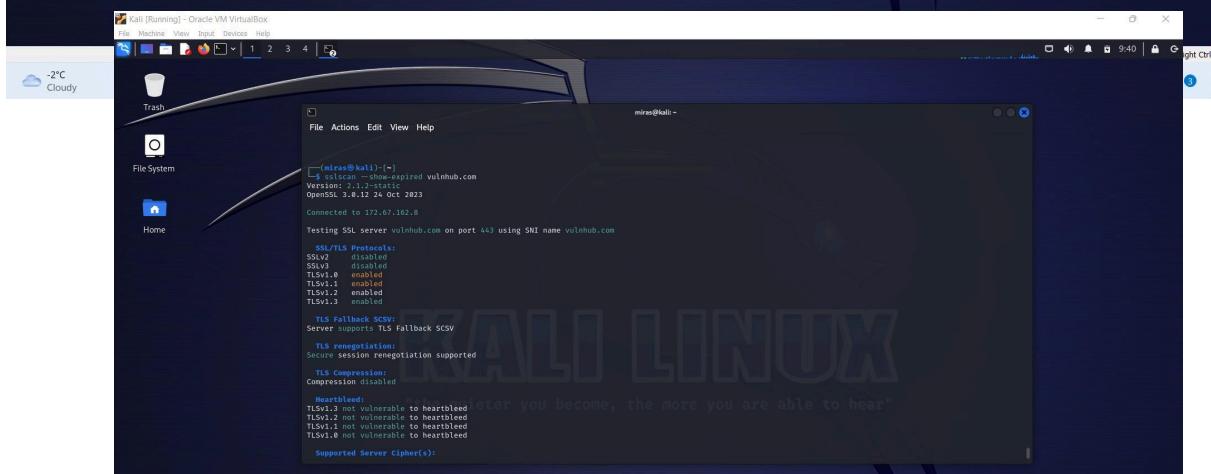
13) Find expired SSL certificates of domains and subdomains.



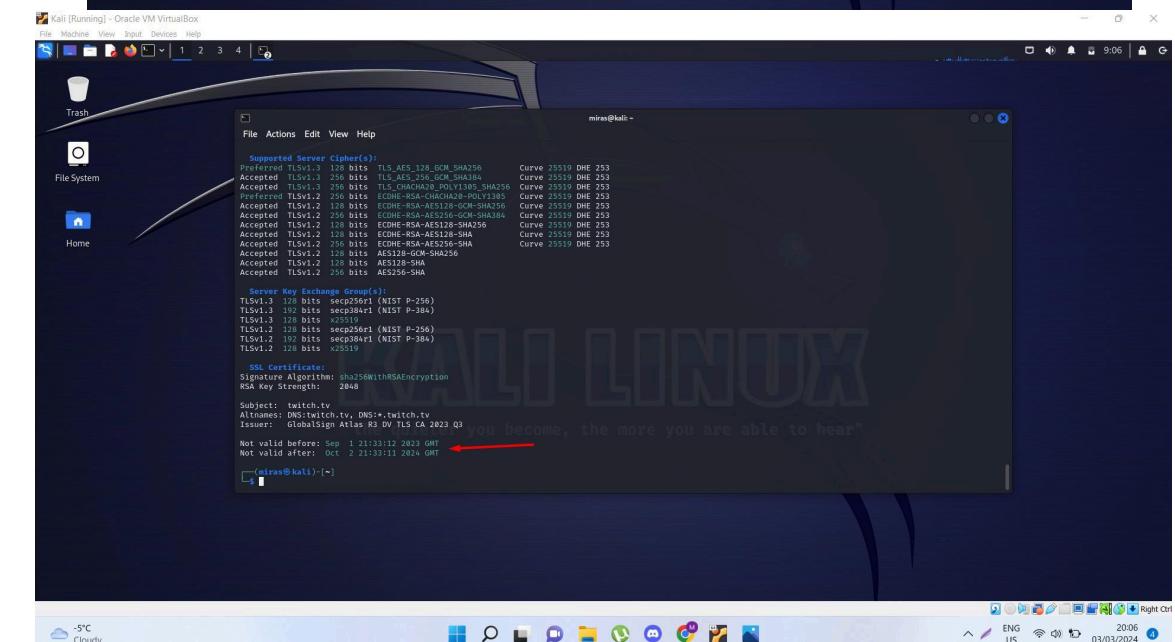
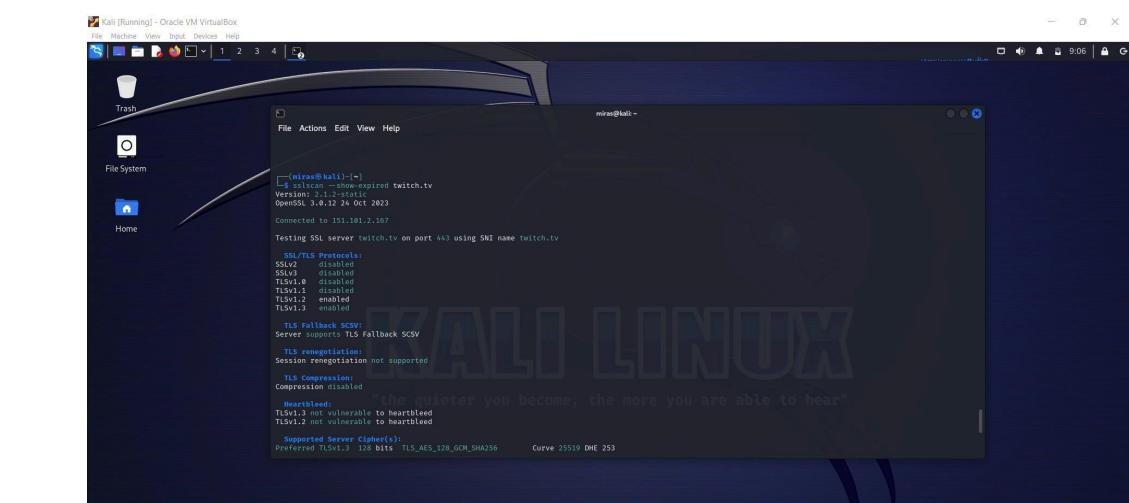
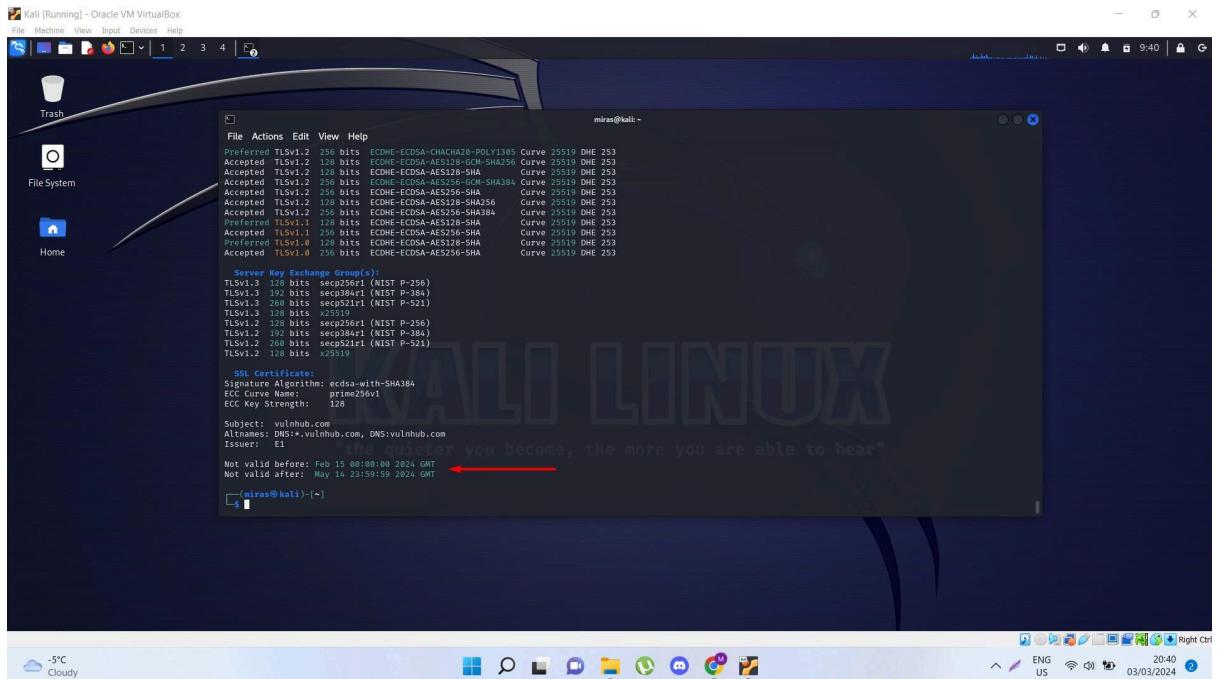
```
(miras@kali)-[~]
└── [root]# curl -v https://imdb.com
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023
Connected to 32.94.237.74
Testing SSL server imdb.com on port 443 using SNI name imdb.com
SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 enabled
TLSv1.1 enabled
TLSv1.2 enabled
TLSv1.3 disabled
TLS Fallback SCSV:
Server supports TLS Fallback SCSV
TLS renegotiation:
Secure session renegotiation supported
TLS Compression:
Compression disabled
Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed
Supported Server Cipher(s):
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
```



```
(miras@kali)-[~]
└── [root]# curl -v https://www.imdb.com
TLSv1.0 not vulnerable to heartbleed
Supported Server Cipher(s):
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 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 TLSv1.2 128 bits AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits AES128-SHA Curve 25519 DHE 253
Preferred TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.1 128 bits AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.0 128 bits AES128-SHA Curve 25519 DHE 253
Server Key Exchange Groups:
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 256 bits secp511r1 (NIST P-521)
TLSv1.2 384 bits secp384r1 (NIST P-384)
TLSv1.2 224 bits x448
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048
Subject: us.dd.imdb.com
AltNames: DNS:imdb.com, DNS:www.imdb.com, DNS:secure.imdb.com, DNS:s.media-imdb.com, DNS:us.dd.imdb.com, DNS:www.imdb.to, DNS:imdb-webservice.amazon.com, DNS:origin-www.imdb.com
Issuer: Amazon RSA 2048 M01
Not valid before: Jan 18 00:00:00 2024 GMT ←
Not valid after: Dec 18 23:59:59 2024 GMT
```

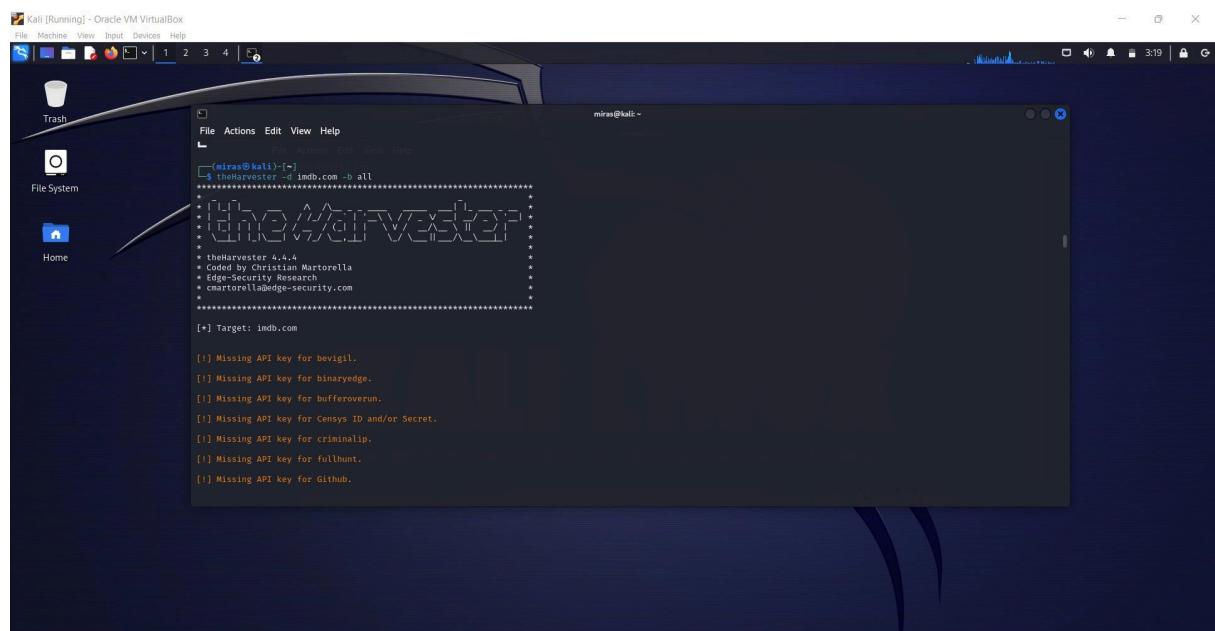


```
(miras@kali)-[~]
└── [root]# curl -v https://vulnhub.com
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023
Connected to 172.0.1.102.8
Testing SSL server vulnhub.com on port 443 using SNI name vulnhub.com
SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 enabled
TLSv1.1 enabled
TLSv1.2 enabled
TLSv1.3 enabled
TLS Fallback SCSV:
Server supports TLS Fallback SCSV
TLS renegotiation:
Secure session renegotiation supported
TLS Compression:
Compression disabled
Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed
Supported Server Cipher(s):
```



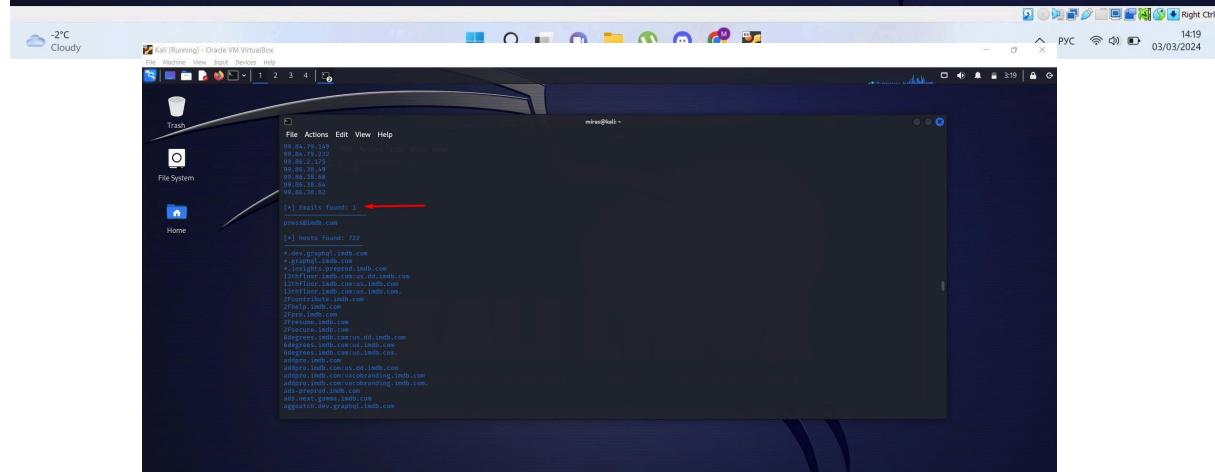
14) Find all emails that are available in the web content of the website.

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



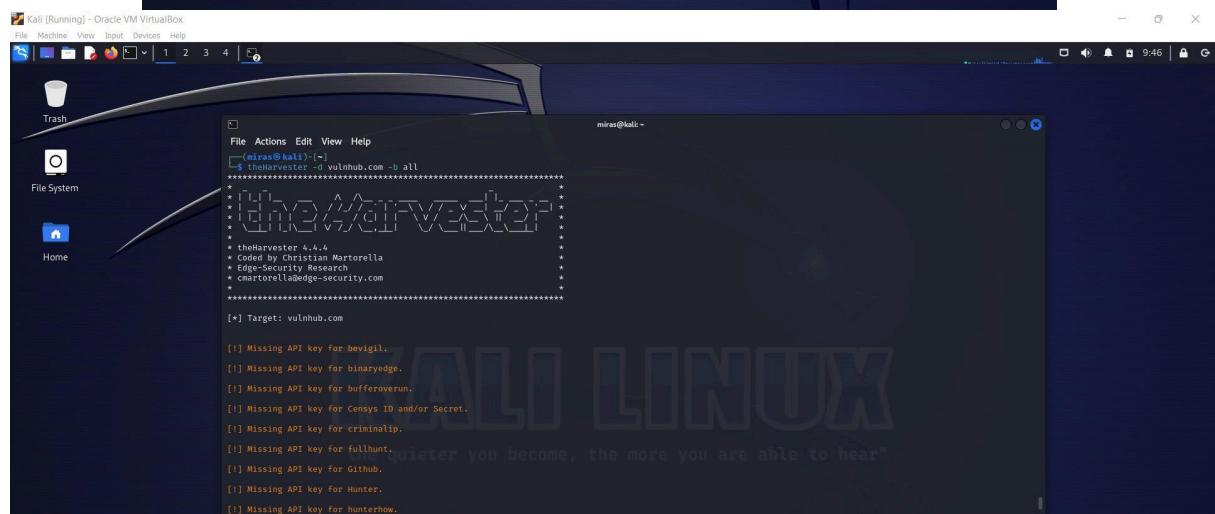
```
miras@kali: ~$ theharvester -d imbd.com -b all
[!] Target: imbd.com

[*] Missing API key for bevigil.
[*] Missing API key for binaryedge.
[*] Missing API key for bufferoverun.
[*] Missing API key for Censys ID and/or Secret.
[*] Missing API key for criminaltrip.
[*] Missing API key for fullhunt.
[*] Missing API key for Github.
```



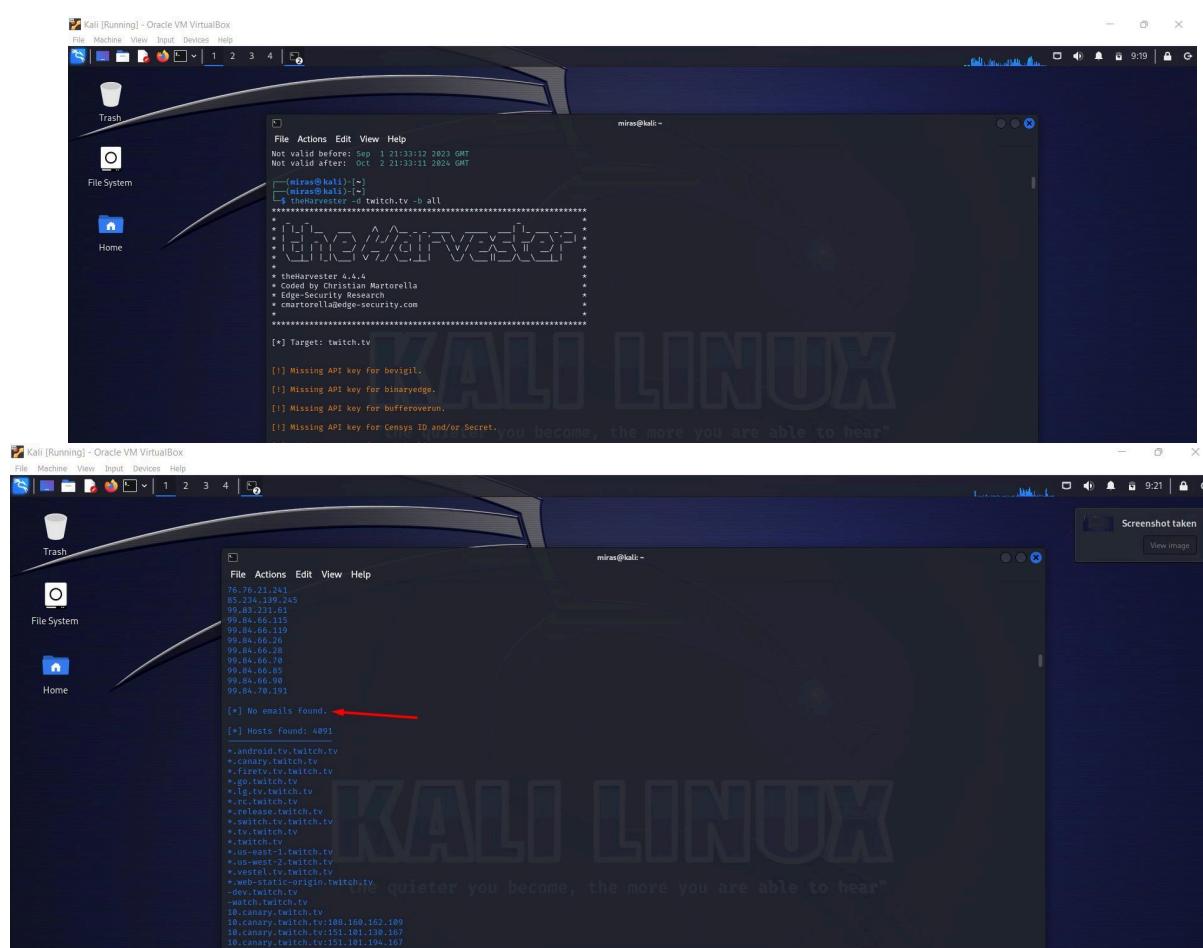
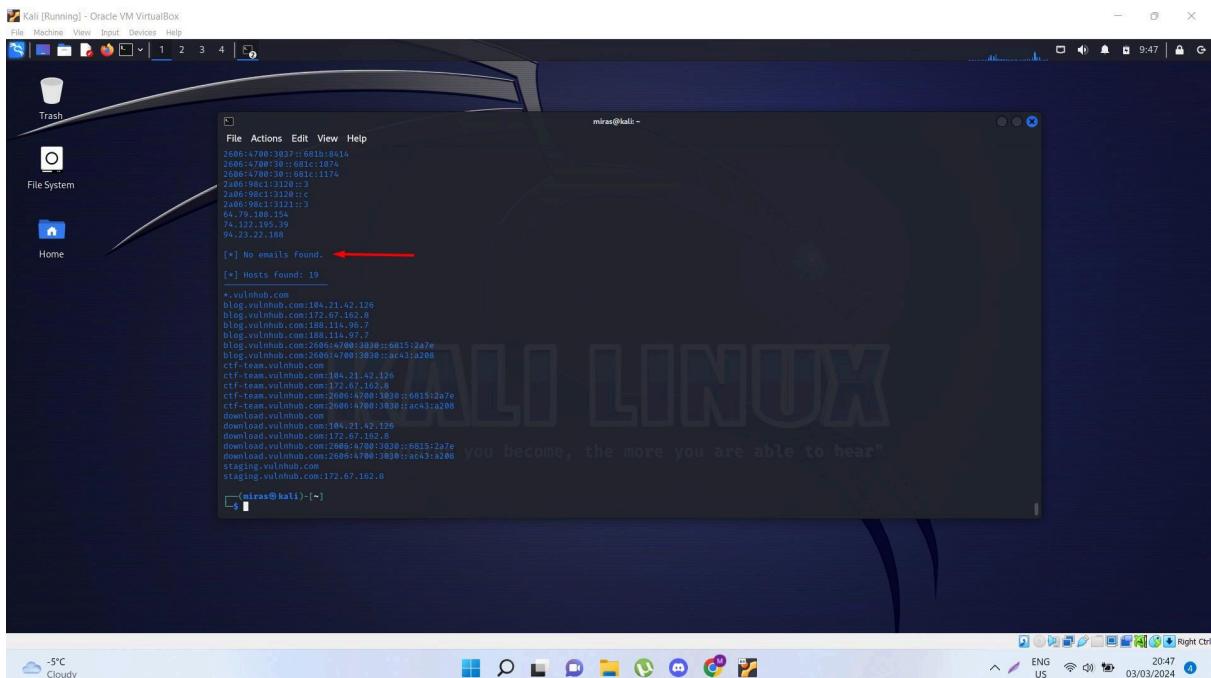
```
miras@kali: ~$ theharvester -d imbd.com -b all
[*] Emails found: 1
```

A red arrow points to the line "[*] Emails found: 1".



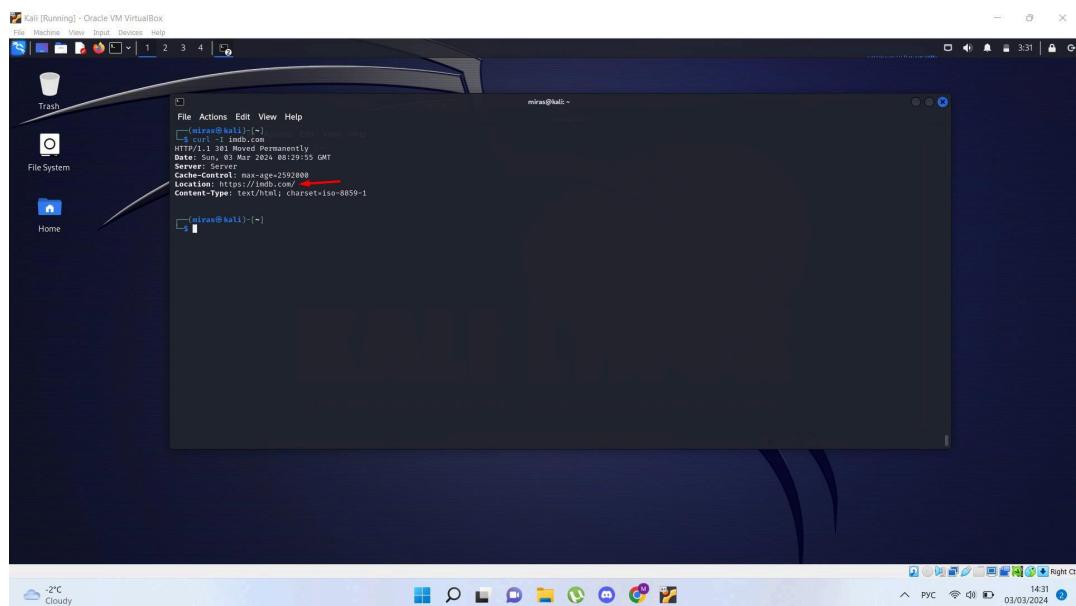
```
miras@kali: ~$ theharvester -d vulnhub.com -b all
[!] Target: vulnhub.com

[*] Missing API key for bevigil.
[*] Missing API key for binaryedge.
[*] Missing API key for bufferoverun.
[*] Missing API key for Censys ID and/or Secret.
[*] Missing API key for criminaltrip.
[*] Missing API key for fullhunt.
[*] Missing API key for Github.
[*] Missing API key for Hunter.
[*] Missing API key for hunterflow.
```

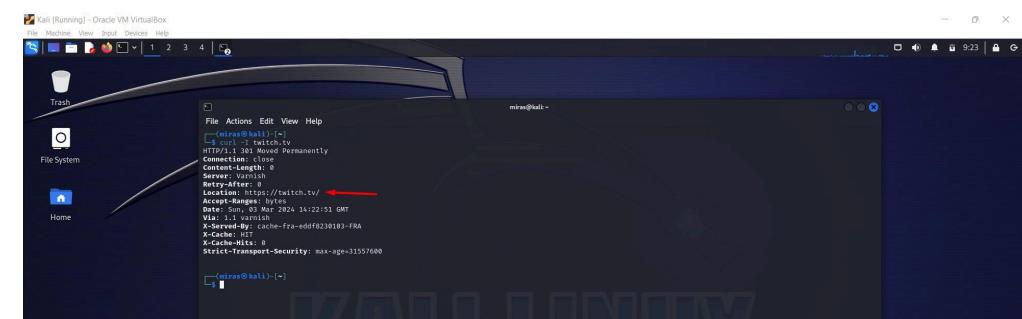


15) Provide the HTTP headers used by domain or subdomains.

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



```
(miras@kali)-[~] curl -I imdb.com
HTTP/1.1 301 Moved Permanently
Date: Sun, 03 Mar 2024 00:29:55 GMT
Server: Server
Content-Type: text/html; charset=iso-8859-1
Location: https://www.imdb.com/
Content-Type: text/html; charset=iso-8859-1
```



```
(miras@kali)-[~] curl -I twitch.tv
HTTP/1.1 301 Moved Permanently
Connection: close
Content-Type: text/html; charset=UTF-8
Server: Varnish
Date: Sun, 03 Mar 2024 14:22:51 GMT
Via: 1.1 varnish
X-Cache: HIT
X-Cache-Hits: 0
Strict-Transport-Security: max-age=31557600
Accept-Ranges: bytes
```

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

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

The image contains three separate screenshots of the HaveIBeenPwned website, each showing the results for a different email address. The top screenshot shows results for 'simeon@imdb.com', indicating 'Oh no — pwned!' with 2 data breaches. The middle screenshot shows results for 'ksann@imdb.com', indicating 'Oh no — pwned!' with 4 data breaches. The bottom screenshot shows results for 'spencer@twitch.tv', indicating 'Oh no — pwned!' with 11 data breaches. Each result page includes a 'Donate' button and social media sharing links.

This screenshot shows the HaveIBeenPwned website for the email address 'yshen@twitch.tv'. It displays 'Oh no — pwned!' with 11 data breaches. The page includes a 'Donate' button and social media sharing links. A note at the bottom left mentions the Adapt breach, which exposed over 9.3M unique records from November 2018.

