

CEH Module 2: Foot Printing and Reconnaissance

Assignment - 01

(Sairaj Mothukuri)

Given Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum Information about the target organization by performing foot printing using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical Information about a target organizationsuch as technology platforms, employee details, Login pages, intranet portals, contact details, etc., which will help you in performing social Engineering and other types of advanced system attacks

Given Lab Objectives:

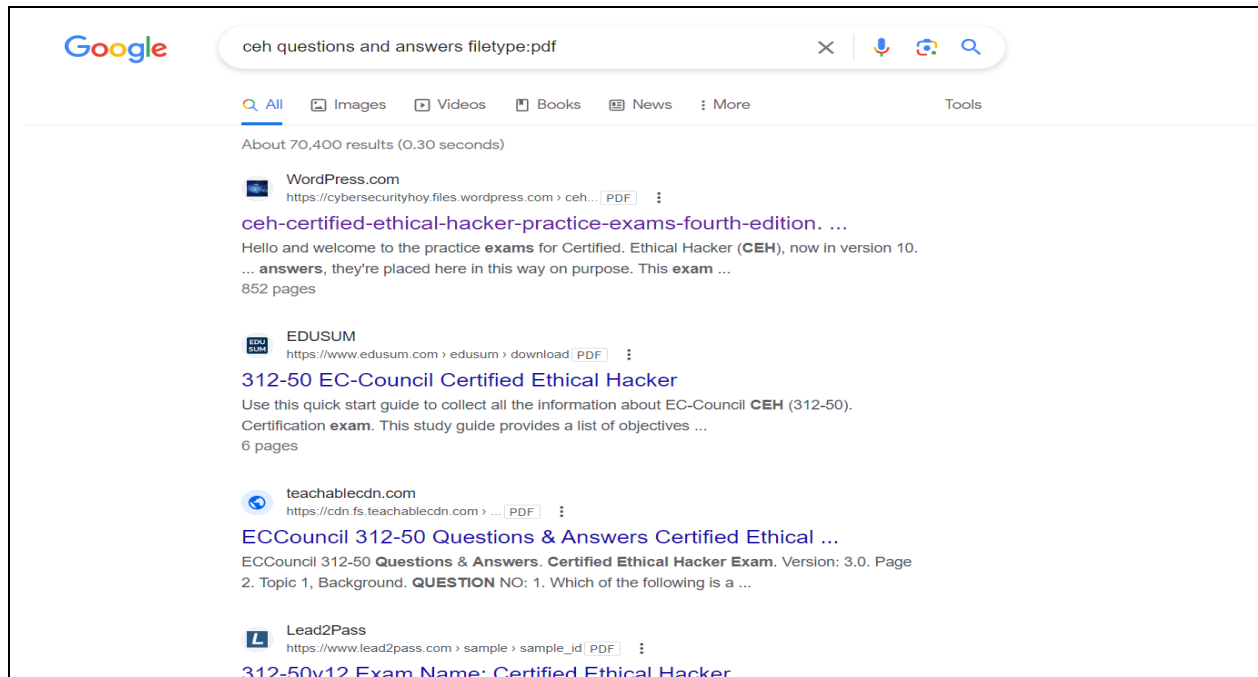
1. Gather information using advanced Google hacking techniques
2. Gather information from video search engines
3. Gather information from FTP search engines
4. Gather information from IoT search engines

Objective – 01

Gather information using advanced Google hacking techniques

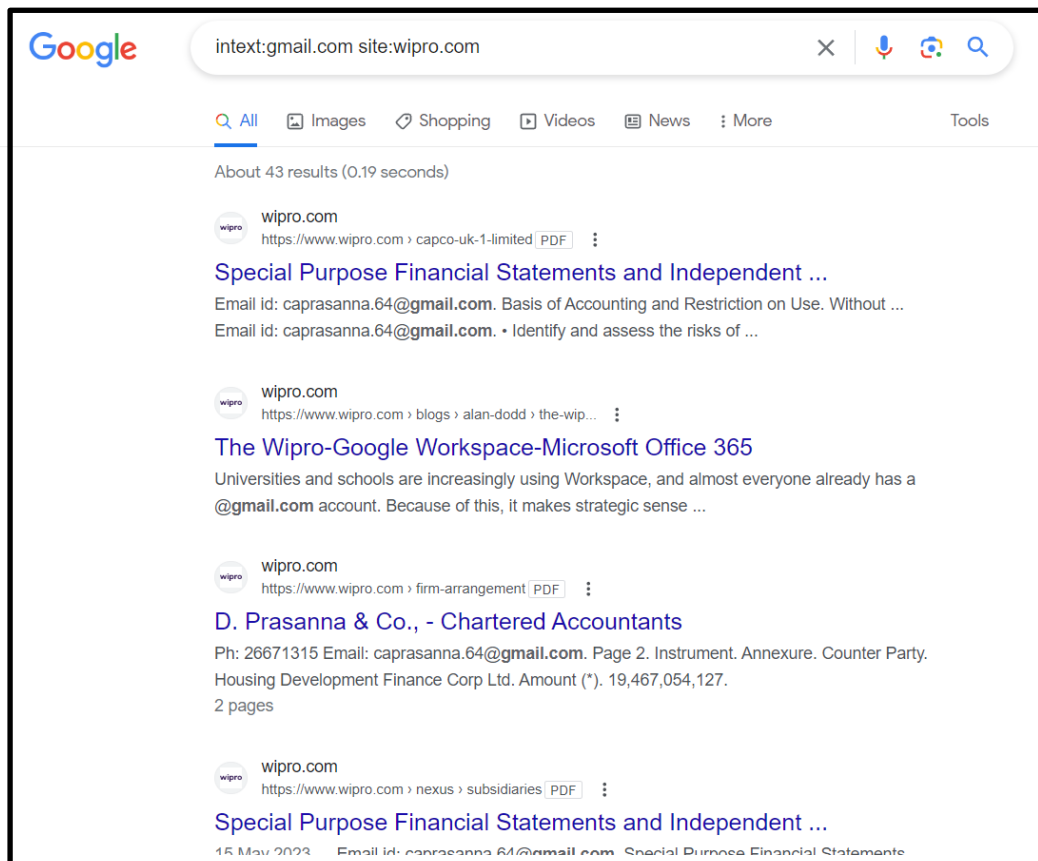
- Finding information using google dorking/hacking commands
- Getting sensitive information of target in internet
- As mentioned in lab scenario here I am using following google dorking/commands
 - Finding PDF files using google dorking/hacking command:
 1. **[CEH question and answers filetype:pdf]**
 - finding emails using google dorking/hacking command:
 2. **[intext:gmail.com site:wipro.com]**
- To gather information using advance google hacking techniques we can use google search engine.

Finding PDF files using google dorking/hacking command:
[CEH question and answers filetype:pdf]



The generated search results are PDF files of my target of using google advance search parameter **"filetype:"**

Finding emails using google dorking/hacking command:
[intext:gmail.com site:wipro



The generated search results are restricted to email related information of my target because are using google dorking/hacked command in advance google search

Objective – 02

Gather information from video search engines

- ❖ Target organization: Yuvasudha Arts
- ❖ Video search engine: You Tube
- ❖ Website for gathering video analytics or information:
MW Metadata



MW Metadata normal grabs singular details about a YouTube video and its uploader, playlist and its creator, or channel.

Submit a link or id to a video, playlist, or channel

<https://youtu.be/rc61YH1PFY?si=gORnOeilPhWrhky8>

Submit

Accepted formats

- https://www.youtube.com/watch?v=video_id
- https://youtube.com/shorts/video_id
- https://youtu.be/video_id
- https://www.youtube.com/playlist?list=playlist_id
- https://www.youtube.com/channel/channel_id
- <https://www.youtube.com/user/username>
- https://www.youtube.com/@channel_handle
- https://www.youtube.com/c/custom_url
- https://www.youtube.com/custom_url
- Also accepts direct ids: video_id, playlist_id, channel_id

Share

Share this result:

<https://mattw.io/youtu>



What happened to export?

Video

The video submitted. [Click here](#) to see detailed property descriptions.



```
{
  "publishedAt": "2024-01-08T10:35:02Z",
  "channelId": "UCoRtbood171AXF2ys7p3gkg",
  "title": "Devara Part-1 | Glimpse - Telugu - NTR | Koratala Siva | Anirudh | 5 April 2024",
  "description": "Watch #Devara Part 1 Glimpse ft. NTR, written & directed by Koratala Siva. The Film's music is composed by Anirudh Ravichander. \n#AllHailTheTig",
  "thumbnails": {
    "default": {
```



Devara Part-1 | Glimpse - Telugu - NTR | Koratala Siva | Anirudh | 5 April 2024

Published by Yuvasudha Arts

Published on [Mon, 08 Jan 2024 10:35:02 GMT](#) (16 days ago) (convert)

Tag(s): [Devara Glimpse \(Telugu\) Part 1](#) [Devara teaser](#) [devara official trailer](#) [NTR](#) [NTR latest teaser](#) [Koratala Siva](#) [Anirudh Ravichander](#) [Devara](#) [Devara Movie](#) [Devara Glimpse](#) [Devara Movie Glimpse](#) [Anirudh](#) [Janhvi Kapoor](#) [Saif Ali Khan](#) [Telugu Movie Devara](#) [Devara Part1](#) [All Hail The Tiger](#) [NTR latest Movie teaser](#) [NTR 30 Movie teaser](#)

✓ Statistics

```
{
  "viewCount": "33968873",
  "likeCount": "792882",
  "favoriteCount": "0",
  "commentCount": "27963"
}
```

YouTube no longer provides the **dislikeCount** since 2021-12-13 (see [more here](#)).

Want dislikes back? Check out the [return-youtube-dislike](#) project!

– Geolocation

```
{}
```

The video does not have recordingDetails.

✓ Status

```
{
  "uploadStatus": "processed",
  "privacyStatus": "public",
  "license": "youtube",
  "embeddable": true,
  "publicStatsViewable": true,
  "madeForKids": false
}
```

This video may be embedded on other websites

This video is not child-directed

✓ Content Details

```
{
  "duration": "PT1M20S",
  "dimension": "2d",
  "definition": "hd",
  "caption": "true",
  "licensedContent": true,
  "contentRating": {},
  "projection": "rectangular"
}
```

The video length was **1m 20s**

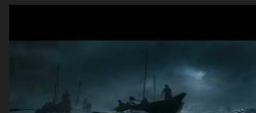
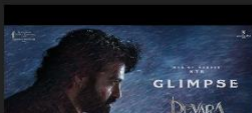
✓ Topic Details

```
{
  "topicCategories": [
    "https://en.wikipedia.org/wiki/Entertainment",
    "https://en.wikipedia.org/wiki/Film"
  ]
}
```

- Entertainment
- Film

? Thumbnails

Reverse image search all four thumbnail images.



✓ Topic Details

```
"/m/02jjt",  
"/m/02vxn"  
],  
"topicCategories": [  
  "https://en.wikipedia.org/wiki/Entertainment",  
  "https://en.wikipedia.org/wiki/Film"  
]  
}
```

- Entertainment
- Film

? More

Check other resources for details or archival.

- Archive.org (search) - @yuvasudhaarts
- Archive.org (search) - UCoRTboOd171AXF2ys7p3gkg
- Archive.org (search) - Yuvasudha Arts
- Archive.org (search) - creator:"Yuvasudha Arts"
- Archive.org (search) - subject:"UCoRTboOd171AXF2ys7p3gkg"
- Archive.org (search) - subject:"Yuvasudha Arts"
- Archive.org - https://www.youtube.com/@yuvasudhaarts
- Archive.org - https://www.youtube.com/@yuvasudhaarts
- Archive.org - https://www.youtube.com/channel/UCoRTboOd171AXF2ys7p3gkg
- Filmot.com - https://filmot.com/channel/UCoRTboOd171AXF2ys7p3gkg
- Google - "@yuvasudhaarts"
- Google - "UCoRTboOd171AXF2ys7p3gkg"
- Google - "Yuvasudha Arts"
- Hobune Archive - UCoRTboOd171AXF2ys7p3gkg
- Socialblade.com - UCoRTboOd171AXF2ys7p3gkg

With the assistance of a MW metadata viewer, I successfully extracted video analytic and essential information related to my target organization.

Objective – 03

Gather information from FTP search engines

- FTP search engines are specialized tools or websites that allow users to search for and discover files and content available on FTP servers across the internet.
- These search engines index the contents of FTP servers, making it easier for users to find specific files or data. Users can search for various types of files, such as software, documents, media, and more.
- FTP search engines can be useful for locating and downloading files that may not be easily accessible through traditional web search engines.

Target Organization: **Facebook**

FTP search engine/website: **NAPLAM FTP Indexer**



With all the words ▾

Searching 1,179,239,264 files (13628.95 TB) in 2,583 FTP servers



With all the words ▾

Showing results 0 to 19 of about 10000 for "facebook"

Order

Related keywords

• [facebook](#) • [packages](#) • [rpm](#) • [Everything](#) • [openbsd](#) • [pidgin](#) • [facebookchat](#) • [68p3](#)
• [tgz](#) • [linux](#) • [aarch64](#) • [pub](#) • [fedora](#) • [releases](#) • [bitlbee](#) • [WWW](#) • [x86](#)
• [tree](#) • [src](#) • [epel](#) • [el8](#) • [purple](#) • [cpan](#) • [modules](#) • [tar](#) • [pub3](#) • [source](#)
• [fc32](#) • [ppc64le](#) • [raspbian](#)

[/openbsd/5.6/packages/mips64el/
pidgin-facebookchat-1.68p3.tgz](#)

109.2 KB Last chequed: 2024-01-23 03:00 Similar files: [\[Browse\]](#)

[/.../linux/fedora/linux/releases/test/39_Beta/Everything/x86_64/os/Packages/b/
bitlbee-facebook-1.2.2-6.fc39.x86_64.rpm](#)

76.9 KB Last chequed: 2024-01-23 03:00 Similar files: [\[Browse\]](#)

[/epel/8/Everything/aarch64/Packages/b/
bitlbee-facebook-1.2.2-1.el8.aarch64.rpm](#)

74.1 KB Last chequed: 2024-01-23 02:59 Similar files: [\[Browse\]](#)

[/pub3/fedora/linux/releases/32/Everything/source/tree/Packages/p/
purple-facebook-0.9.6-4.fc32.src.rpm](#)

494.2 KB Last chequed: 2024-01-23 02:59 Similar files: [\[Browse\]](#)

[/openbsd/5.7/packages/amd64/
pidgin-facebookchat-1.68p3.tgz](#)

115.9 KB Last chequed: 2024-01-23 02:59 Similar files: [\[Browse\]](#)

[/openbsd/5.7/packages/i386/
pidgin-facebookchat-1.68p3.tgz](#)

110.0 KB Last chequed: 2024-01-23 02:58 Similar files: [\[Browse\]](#)

[/epel/8/Everything/ppc64le/Packages/b/](#)

70.8 KB

**This is how I collected information about the target organization, using FTP
search engines like NAPALM FTP indexer**

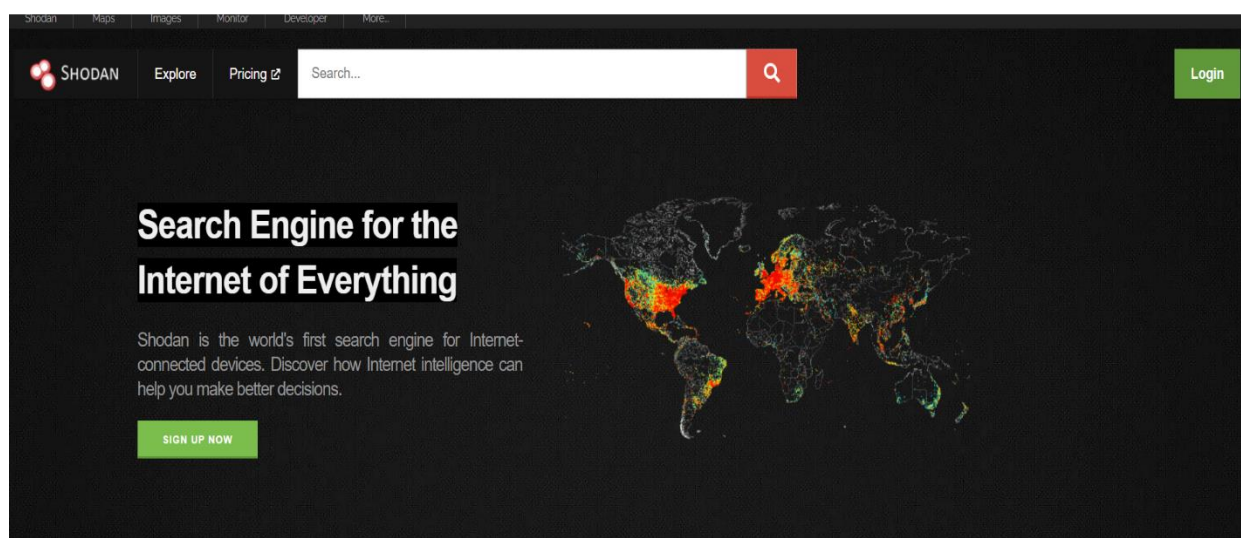
Objective – 04

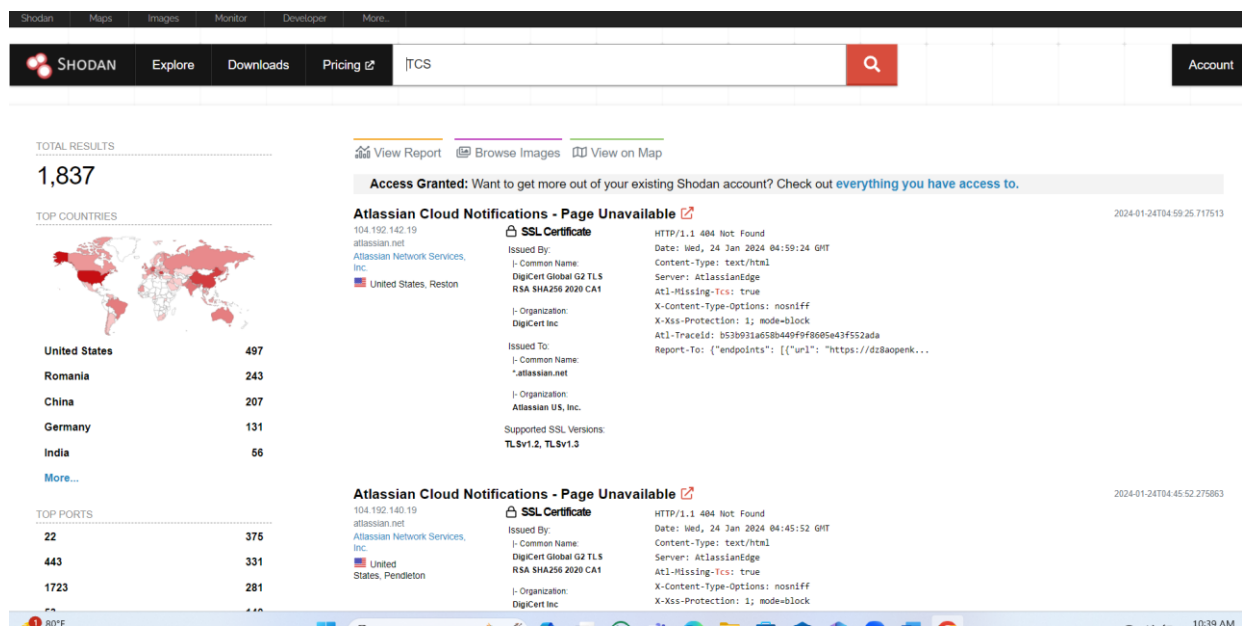
Gather information from IoT search engines

- ❖ The Internet of Things (IoT) refers to a network of physical objects, devices, vehicles, and other items that are embedded with sensors, software, and connectivity, allowing them to collect and exchange data over the internet.
- ❖ Unlike traditional search engines used for web content, IoT search engines are specialized tools designed to discover and access IoT devices and their data on the internet. These search engines can help users locate and interact with IoT devices, which can be especially useful for developers, researchers, and organizations involved in IoT-related projects

Target Organization: **TCS**

IoT Search Engine: **SHODAN (shodan.io)**





This is how I gathered vulnerable information about my target organization using IoT search engines (**SHODAN**).

Submitted By

Sairaj mothukuri

sairajmothukuri28@gmail.com