CEH Module 2: Foot Printing and Reconnaissance
Assignment - 01
(Marepalli Rakesh)

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 organization such 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

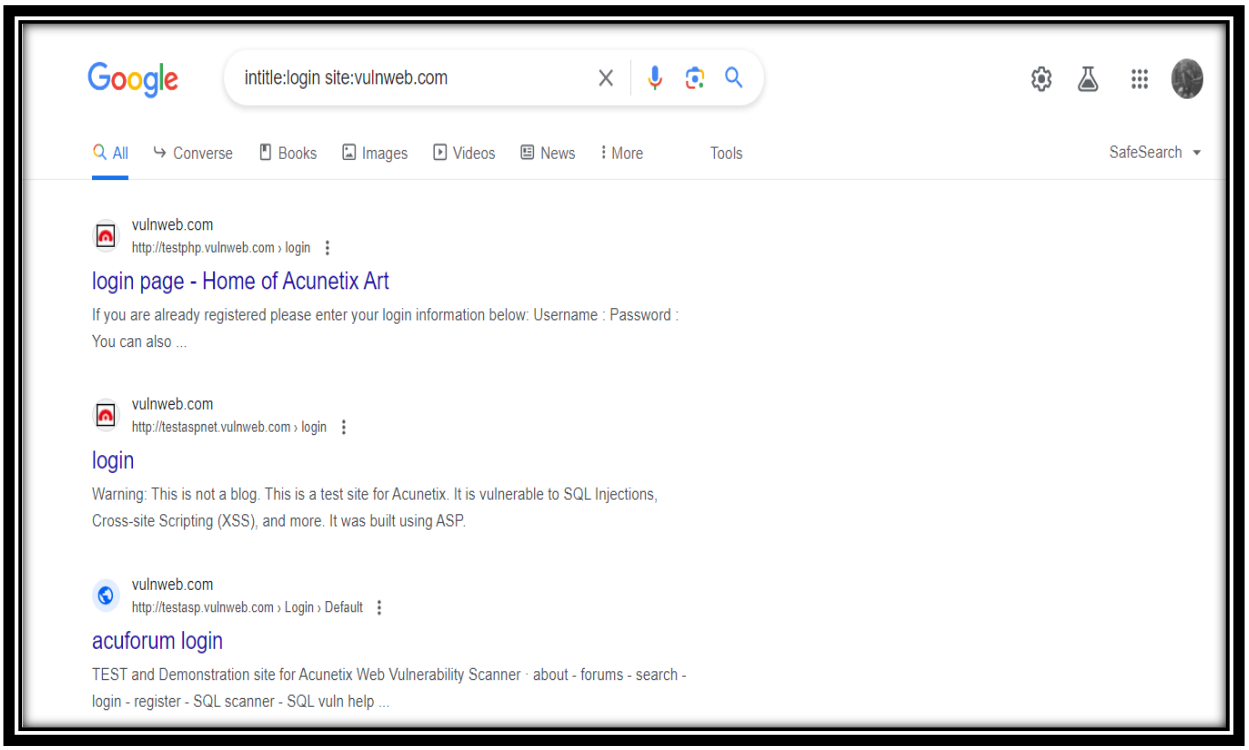
:

- Advanced Google hacking often referred to as "Google dorking" or "Google hacking," is a technique that involves using advanced search operators and specific search queries to find sensitive or hidden information on the internet, primarily through the Google search engine. It's a form of information retrieval and reconnaissance that can be used for both legitimate and malicious purposes, depending on the intent of the user.
- To gather critical information using advanced google hacking techniques in this case I am considering multiple websites as my target because justifying lab scenario with one single target is a little bit complex (ex: www.intellipaat.com. www.vulnweb.com. www.jntuh.ac.in and etc.)
- As mentioned in lab scenario here I am using below following search queries/commands to gather critical information about my target organizations such as technology platform, employee details, login pages, intranet portals, contact details etc.

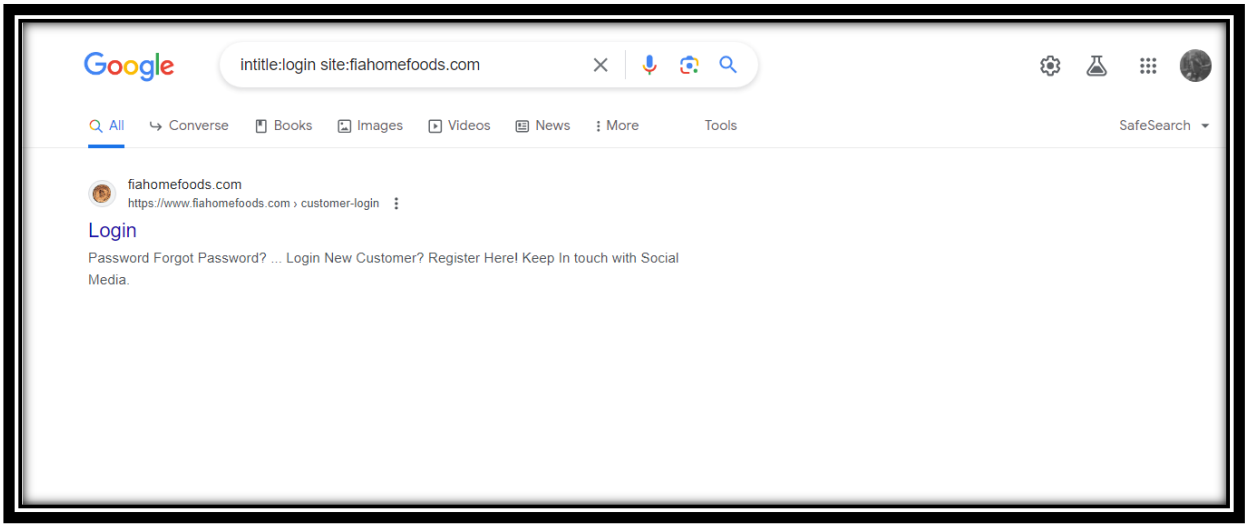
Finding login pages using google dorking/hacking command :(intitle:login site:vulnweb.com)
Finding emails of a target organization using command :(intext:gmail.com site:jntuh.ac.in)
Finding contact information about the target using command :(inurl:contact site:jntuh.ac.in)
Finding digital files about the target using command: (site:Intellipaat.com filetype:pdf)

Finding login pages using google dorking/hacking command: (intitle:login site:vulnweb.com)

To find the login pages of my target org using advanced google hacking techniques first I opened google search engine. After that I used the command (intitle:login site:vulnweb.com) on search bar. This search command uses **intitle** and **site** google advance operators which restrict results to pages on vulnweb.com website that contain login pages. As shown in below



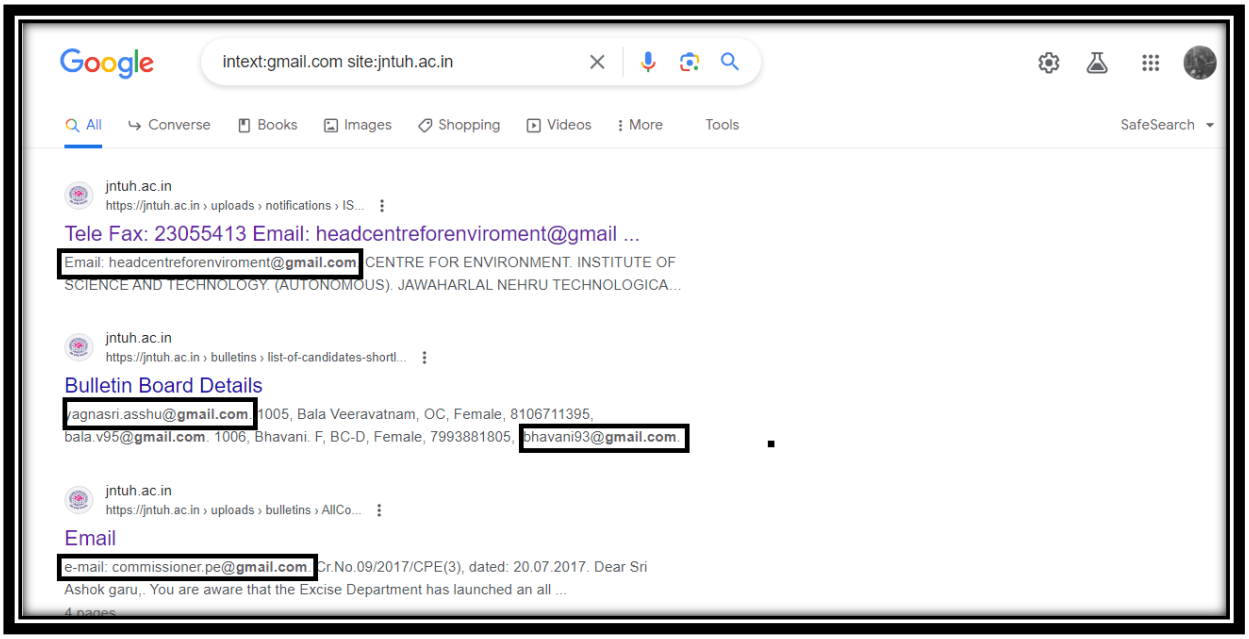
The generated search results are restricted to login pages of my target organization because of we are using google advanced search parameter intitle and site



Those google search results takes me to the login pages of target organizations

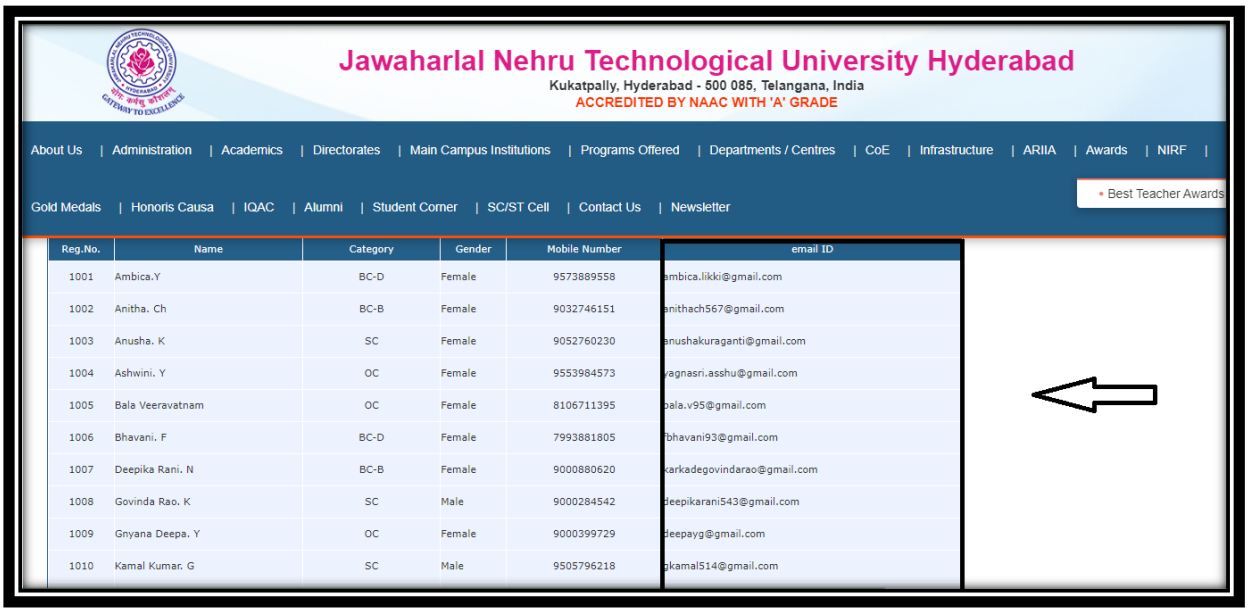
Finding emails of a target organization using command: (intext:gmail.com site:jntuh.ac.in)

To find the emails of my target org using advanced google hacking techniques first I opened my google search engine. After that I used the search bar of google and used the command (intext:gmail.com site:jntuh.ac.in) and google delivered the results which are shown below



The generated search results are restricted to emails related information of my target organization because of we are using google advanced search parameter intext and site

When I go inside the 2nd search result (bulletin board details) I found below result

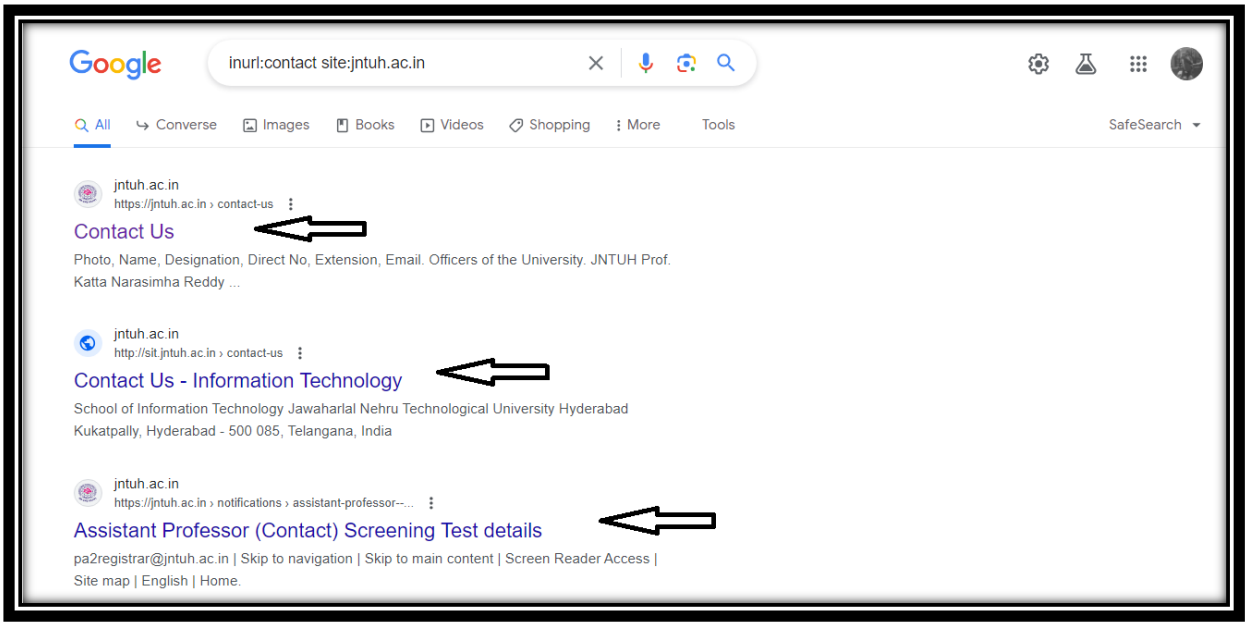


Reg.No.	Name	Category	Gender	Mobile Number	email ID
1001	Ambica.Y	BC-D	Female	9573889558	ambica.likki@gmail.com
1002	Anitha. Ch	BC-B	Female	9032746151	anithach567@gmail.com
1003	Anusha. K	SC	Female	9052760230	anushakuraganti@gmail.com
1004	Ashwini. Y	OC	Female	9553984573	vagnasri.asshu@gmail.com
1005	Bala Veeravatnam	OC	Female	8106711395	bala.v95@gmail.com
1006	Bhavani. F	BC-D	Female	7993881805	bhavani93@gmail.com
1007	Deepika Rani. N	BC-B	Female	9000880620	karkadegovindarao@gmail.com
1008	Govinda Rao. K	SC	Male	9000284542	deepikarani543@gmail.com
1009	Gnyana Deepa. Y	OC	Female	9000399729	deepayg@gmail.com
1010	Kamal Kumar. G	SC	Male	9505796218	gkamal514@gmail.com

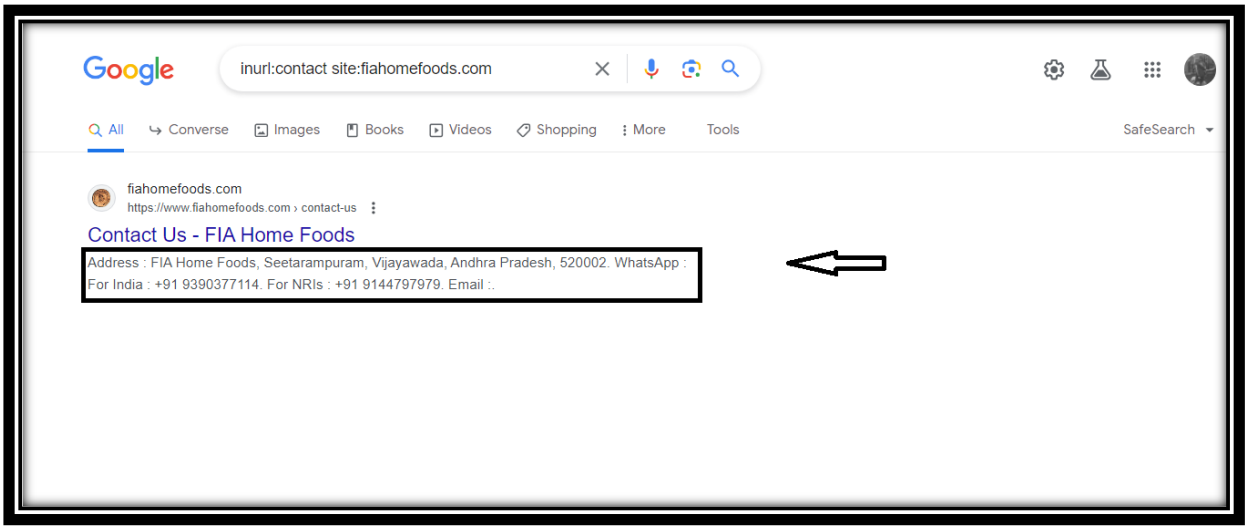
That's how I used advanced google hacking techniques to get emails of my target organization

Finding contact information about the target using command: (inurl:contact site:jntuh.ac.in)

To find the contact information of my target organization using advanced google hacking techniques first I opened my google search engine. After that I used the search bar of google and used the command (inurl:contact site:jntuh.ac.in) and google delivered the results which are shown below



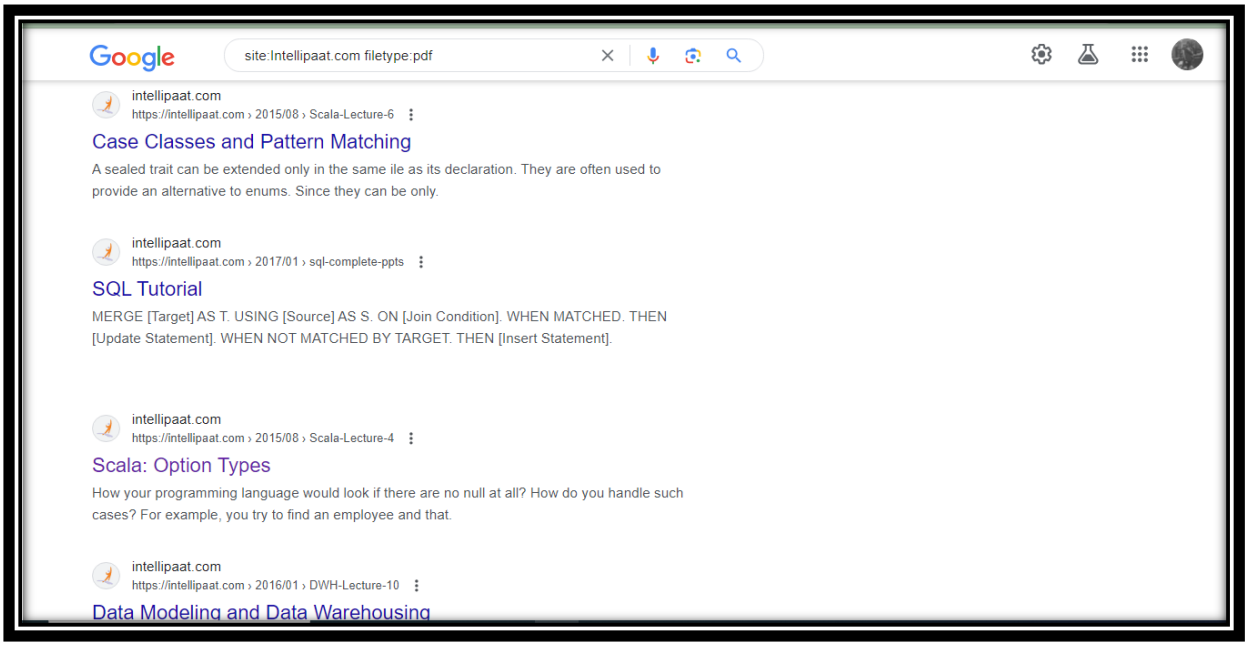
The generated search results are restricted to contact of my target organization because of we are using google advanced search parameter inurl and site



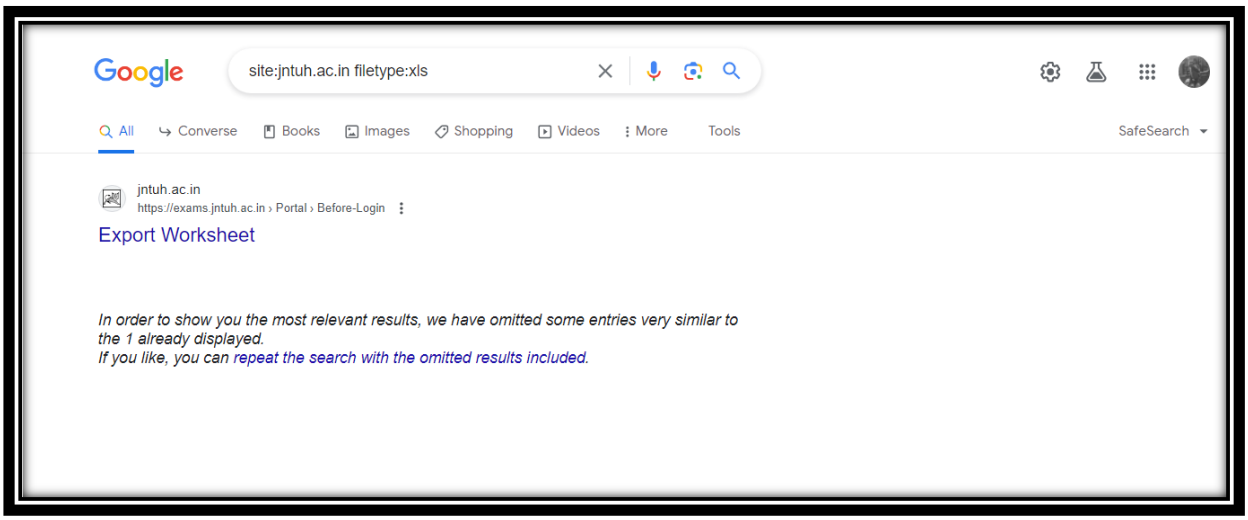
That's how I used advanced google hacking techniques to get contact information of my target organizations

Finding digital files about the target using command:
(site:Intellipaat.com filetype:pdf)

To find the digital files of my target organization using advanced google hacking techniques first I opened my google search engine. After that I used the search bar of google and used the command (site:intellipaat.com filetype:pdf) and google delivered the results which are shown below



The generated search results are restricted to different files of my target organization because of we are using google advanced search parameter file type (it maybe pdf, xls.txt.doc) and site



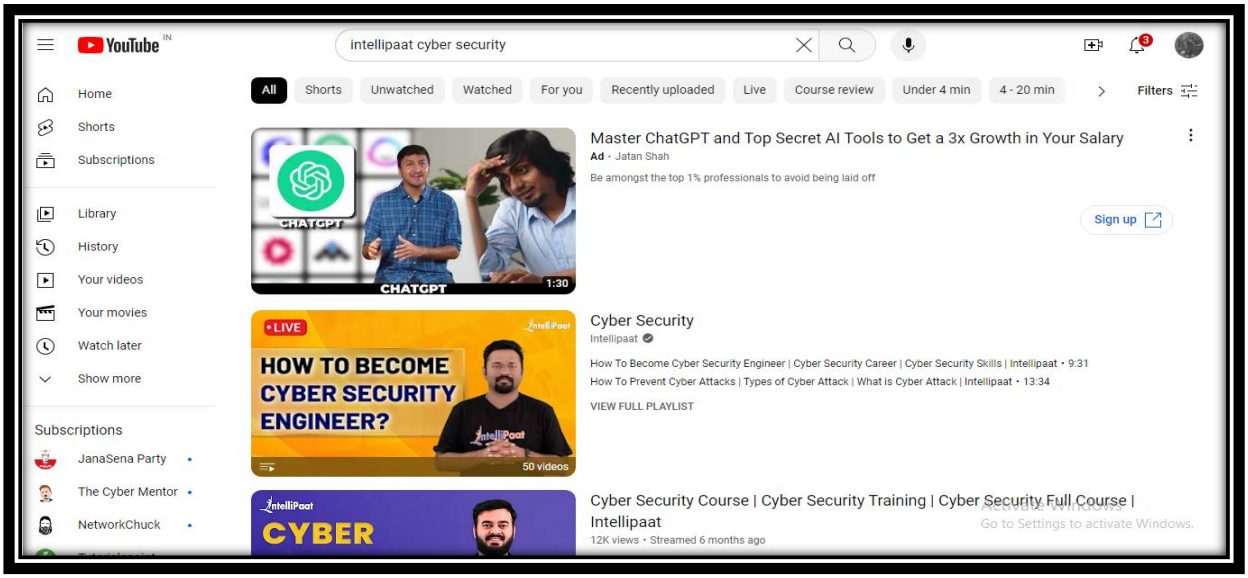
That’s how I used advanced google hacking techniques to get digital files of my target organizations

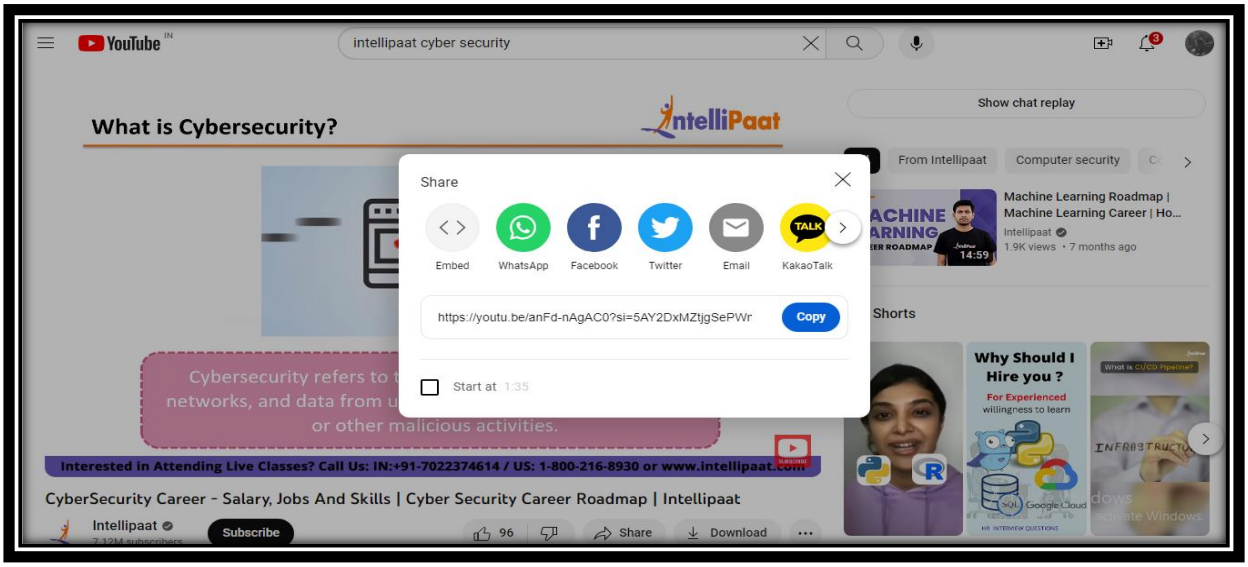
Objective – 02

Gather information from video search engines

- Target Organization: Intellipaat
- Video Search Engine: YouTube
- Website for Gathering Video Analytics: MW Metadata (https://mattw.io/youtube-metadata/)

1. I began by opening my web browser and navigating to YouTube.
2. Using the YouTube search bar, I looked up videos related to the organization Intellipaat and selected one of interest. I then copied the URL for that video.
3. I proceeded to access a YouTube metadata viewer through a provided link.
4. In the metadata viewer, I pasted the copied video URL into the search bar and clicked the "submit" button.
5. The metadata viewer promptly displayed a wealth of information, including details such as the upload time, status, likes, localization, and content specifics for the selected video.





01 MW Metadata Normal Bulk

Dark

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/anFd-nAgAC0?si=wUHo8wx0R8S5YBCP

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:

What happened to export?

Snippet


```
{
    "publishedAt": "2023-02-12T12:30:10Z",
    "channelId": "UCCktnahuRFYIBtNnKT5IYyg",
    "title": "CyberSecurity Career - Salary, Jobs And Skills | Cyber Security Career Roadmap | Intellipaat",
    "description": "▶ Intellipaat's Advanced Certification in Cyber Security: https://intellipaat.com/cyber-security-eict-iit-guwahati/\n\n
    "thumbnails": {
        "default": {
```


CyberSecurity Career - Salary, Jobs And Skills | Cyber Security Career Roadmap | Intellipaat

Published by Intellipaat

Statistics


```
{
    "viewCount": "2843",
    "likeCount": "96",
    "favoriteCount": "0",
    "commentCount": "12"
}
```


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": false,
    "madeForKids": false
}
```

This video may be embedded on other websites

This video is not child-directed

Livestream Details


```
{
    "actualStartTime": "2023-02-12T12:30:10Z",
    "actualEndTime": "2023-02-12T12:47:53Z",
    "scheduledStartTime": "2023-02-12T12:30:00Z"
}
```


The stream started on Sun, 12 Feb 2023 12:30:10 GMT (8 months ago) (convert)

The stream ended on Sun, 12 Feb 2023 12:47:53 GMT (8 months ago) (convert)

The stream was 10s late to start

The stream is over. It's length was 17m 43s

Localizations


```
{
    "en": {
        "description": "▶ Intellipaat's Advanced Certification in Cyber Security: https://intellipaat.com/cyber-security-eict-iit-guwahati/\n\
        "title": "CyberSecurity Career - Salary, Jobs And Skills | Cyber Security Career Roadmap | Intellipaat"
    }
}
```


Localizations for...

- EN which is English

Content Details


```
{
    "duration": "PT15M48S",
    "dimension": "2d",
    "definition": "hd",
    "caption": "false",
    "licensedContent": false,
    "contentRating": {},
    "projection": "rectangular"
```


The video length was 15m 48s

Topic Details

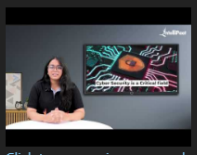

```
{
    "topicCategories": [
        "https://en.wikipedia.org/wiki/Knowledge",
        "https://en.wikipedia.org/wiki/Technology"
    ]
}
```


- Knowledge
- Technology

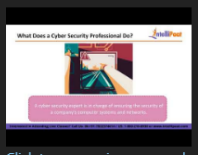
Thumbnails

Reverse image search all four thumbnail images.

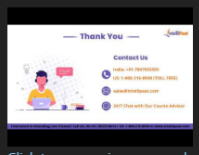
Click to reverse image search



Click to reverse image search



Click to reverse image search



Click to reverse image search

More

Check other resources for details or archival.

- Archive.org (details) - youtube-anFd-nAgAC0
- Archive.org (direct video raw) - anFd-nAgAC0
- Archive.org (direct video wayback-header) - anFd-nAgAC0
- Archive.org (search) - CyberSecurity Career - Salary, Jobs And Skills | Cyber Security Career Roadmap | Intellipaat
- Archive.org (web) - https://www.youtube.com/watch?v=anFd-nAgAC0
- Filmot.com - https://filmot.com/video/anFd-nAgAC0
- GhostArchive.org - anFd-nAgAC0
- Google - "CyberSecurity Career - Salary, Jobs And Skills | Cyber Security Career Roadmap | Intellipaat"
- Google - "anFd-nAgAC0"
- Hobune Archive - anFd-nAgAC0

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

Objective – 03

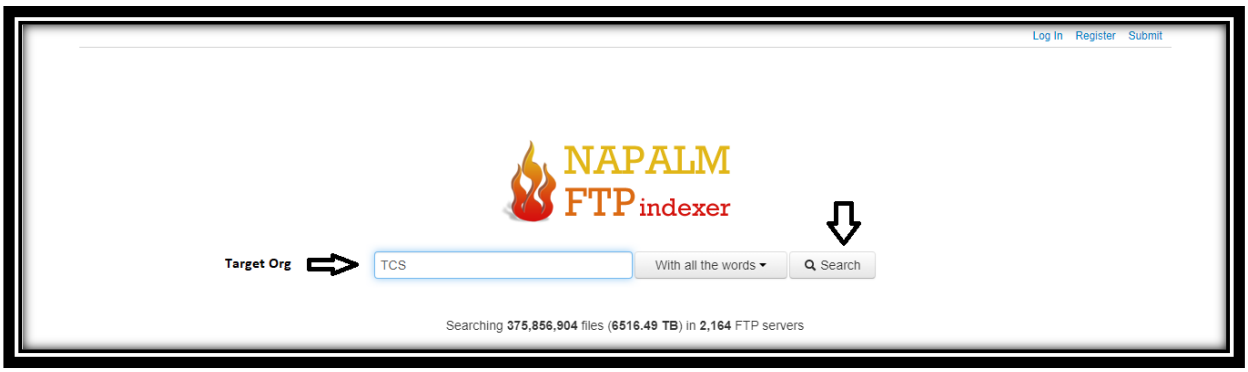
Gather information from FTP search engines

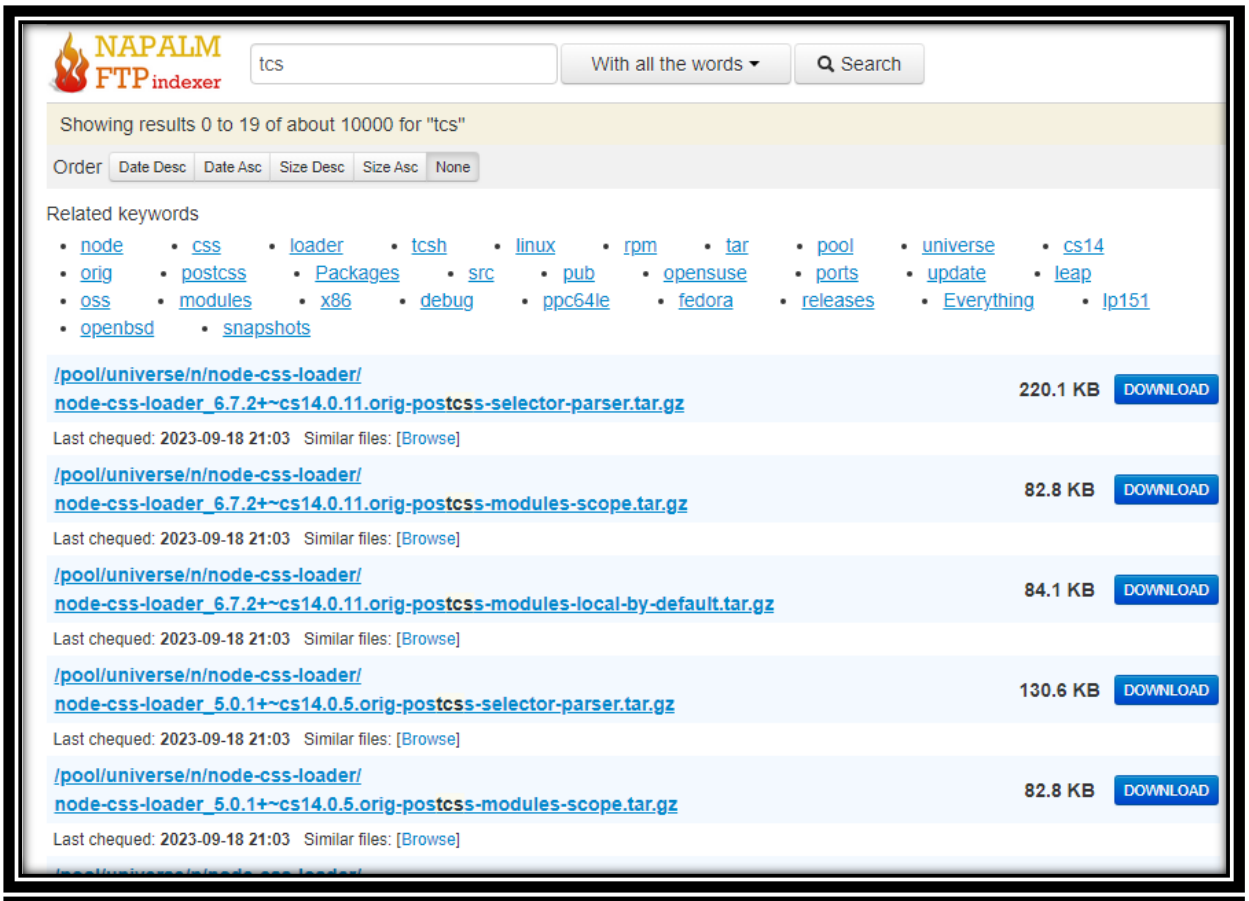
- FTP search engines are specialized tools or websites that allow users to search for and discover files and content available on FTP servers across the internet.
- These search engines index the contents of FTP servers, making it easier for users to find specific files or data. Users can search for 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.

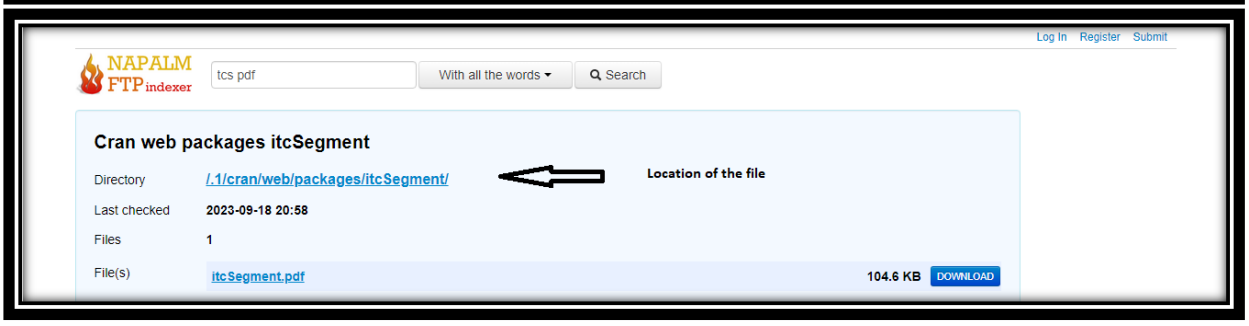
Target Organization: **TCS**

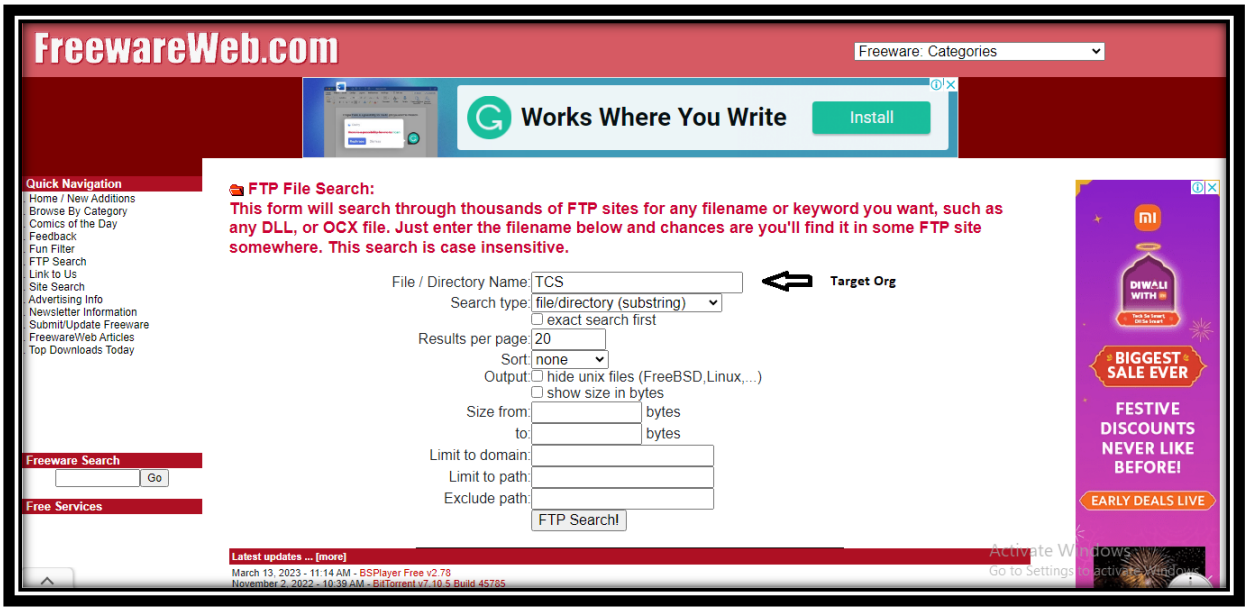
FTP search engine/website: **NAPLAM FTP Indexer & freeware web ftp search**

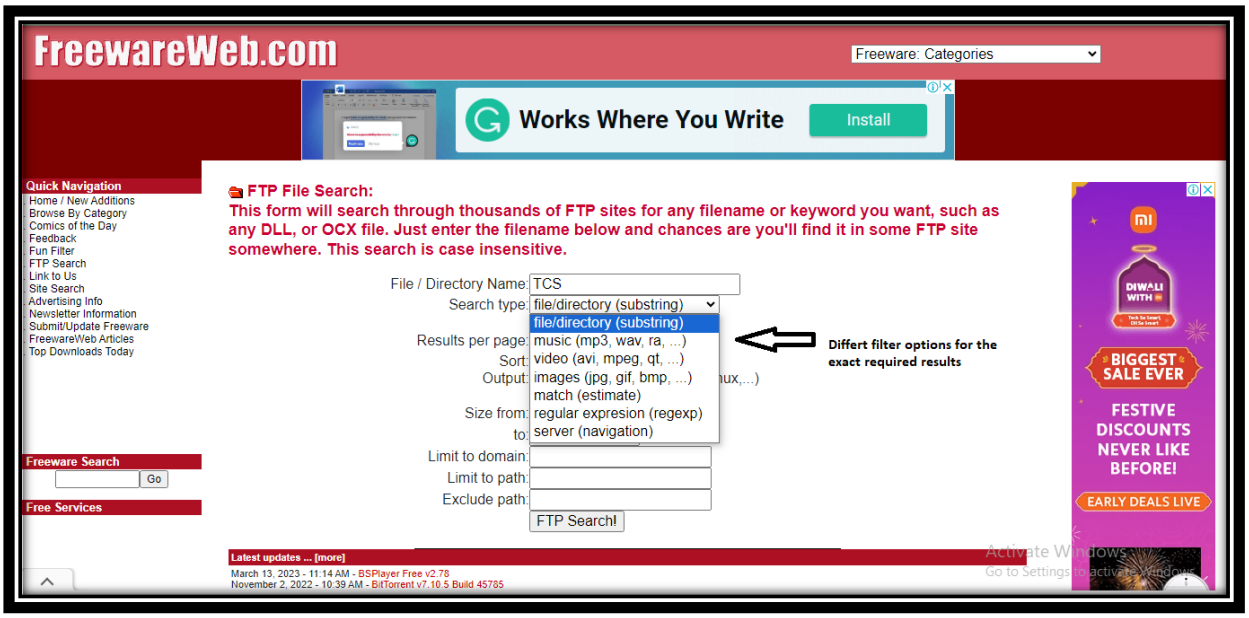
1. I opened my web browser and accessed the Napalm FTP Index.
2. In the Napalm FTP Index search bar, I entered "TCS," my target organization.
3. I successfully located a variety of files, including images, videos, and documents related to TCS, all available on an FTP server. I also discovered the directories where these files were stored.
4. I repeated the process using Freeware Web FTP Search.
5. This time, I noticed an added feature: the ability to filter results by category, including images, videos, music files, and more.

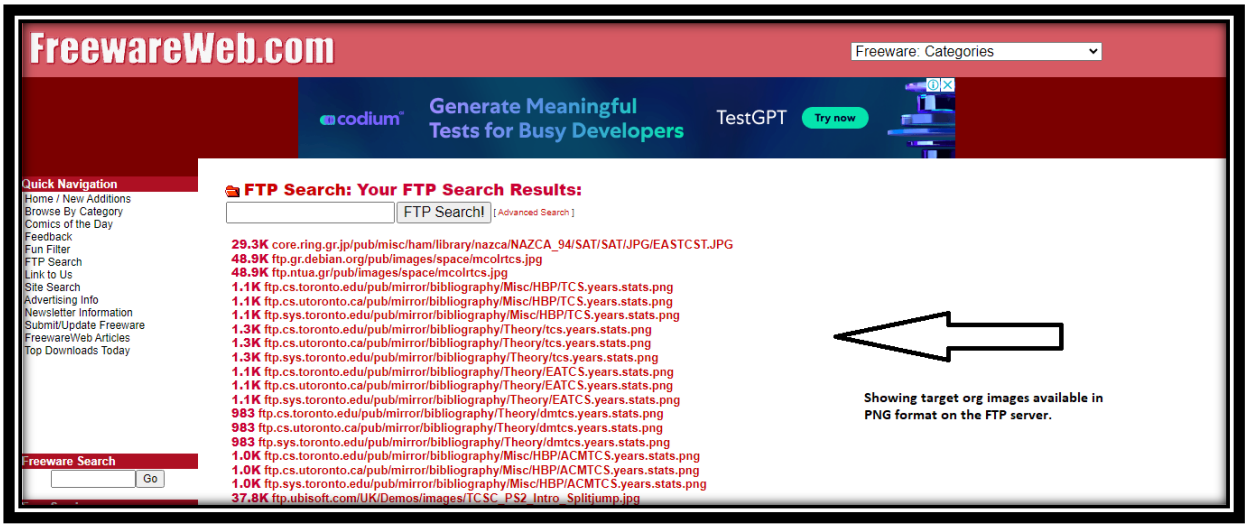



NAPALM FTP indexer
tcs
With all the words
Search
Showing results 0 to 19 of about 10000 for "tcs"
Order Date Desc Date Asc Size Desc Size Asc None
Related keywords
node css loader tcsh linux rpm tar pool universe cs14
orig postcss Packages src pub opensuse ports update leap
oss modules x86 debug ppc64le fedora releases Everything lp151
openbsd snapshots
/pool/universe/n/node-css-loader/
node-css-loader_6.7.2+~cs14.0.11.orig-postcss-selector-parser.tar.gz
220.1 KB DOWNLOAD
Last chequed: 2023-09-18 21:03 Similar files: [Browse]
/pool/universe/n/node-css-loader/
node-css-loader_6.7.2+~cs14.0.11.orig-postcss-modules-scope.tar.gz
82.8 KB DOWNLOAD
Last chequed: 2023-09-18 21:03 Similar files: [Browse]
/pool/universe/n/node-css-loader/
node-css-loader_6.7.2+~cs14.0.11.orig-postcss-modules-local-by-default.tar.gz
84.1 KB DOWNLOAD
Last chequed: 2023-09-18 21:03 Similar files: [Browse]
/pool/universe/n/node-css-loader/
node-css-loader_5.0.1+~cs14.0.5.orig-postcss-selector-parser.tar.gz
130.6 KB DOWNLOAD
Last chequed: 2023-09-18 21:03 Similar files: [Browse]
/pool/universe/n/node-css-loader/
node-css-loader_5.0.1+~cs14.0.5.orig-postcss-modules-scope.tar.gz
82.8 KB DOWNLOAD
Last chequed: 2023-09-18 21:03 Similar files: [Browse]


Log In Register Submit
NAPALM FTP indexer
tcs pdf
With all the words
Search
Cran web packages itcSegment
Directory /.1/cran/web/packages/itcSegment/
Location of the file
Last checked 2023-09-18 20:58
Files 1
File(s) itcSegment.pdf 104.6 KB DOWNLOAD


FreewareWeb.com
Freeware: Categories
Works Where You Write
Install
Quick Navigation
Home / New Additions
Browse By Category
Comics of the Day
Feedback
Fun Filter
FTP Search
Link to Us
Site Search
Advertising Info
Newsletter Information
Submit/Update Freeware
FreewareWeb Articles
Top Downloads Today
Freeware Search
Go
Free Services
FTP File Search:
This form will search through thousands of FTP sites for any filename or keyword you want, such as any DLL, or OCX file. Just enter the filename below and chances are you'll find it in some FTP site somewhere. This search is case insensitive.
File / Directory Name: TCS
Target Org
Search type: file/directory (substring)
exact search first
Results per page: 20
Sort: none
Output: hide unix files (FreeBSD,Linux,...)
show size in bytes
Size from: bytes
to: bytes
Limit to domain:
Limit to path:
Exclude path:
FTP Search!
Latest updates ... [more]
March 13, 2023 - 11:14 AM - BSPlayer Free v2.78
November 2, 2022 - 10:39 AM - BitTorrent v7.10.5 Build 45785
BIGGEST SALE EVER
FESTIVE DISCOUNTS NEVER LIKE BEFORE!
EARLY DEALS LIVE
Activate Windows
Go to Settings to activate Windows.





This is how I collected information about the target organization, using FTP search engines like Napalm and Freeware Web.

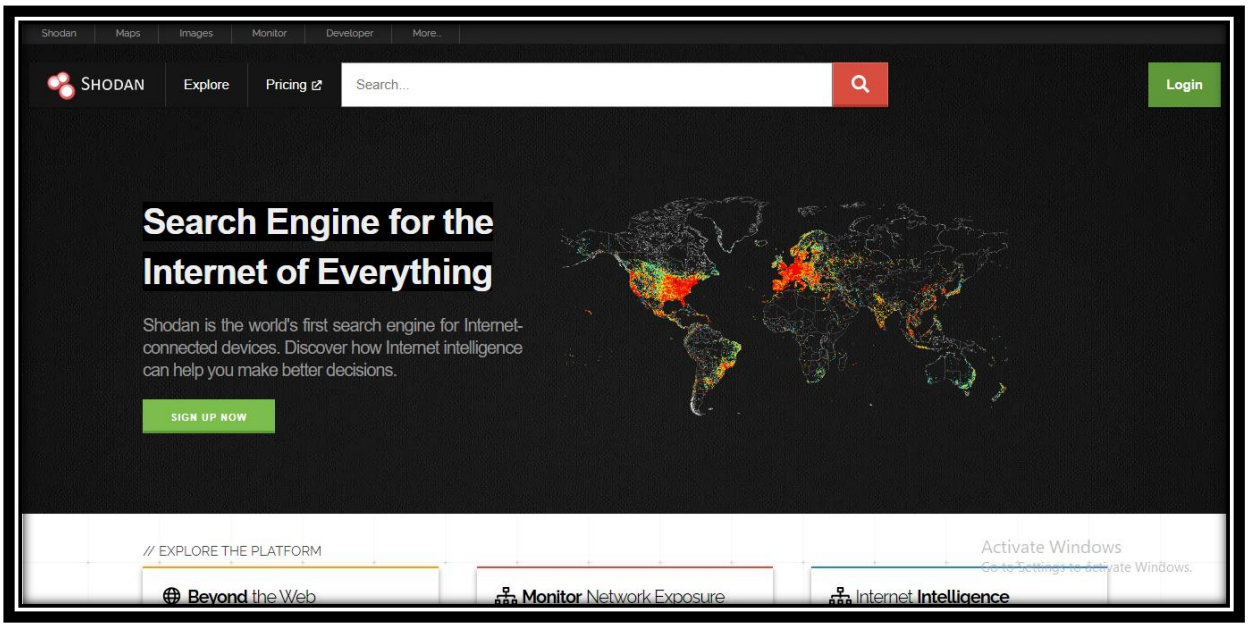
Objective – 04

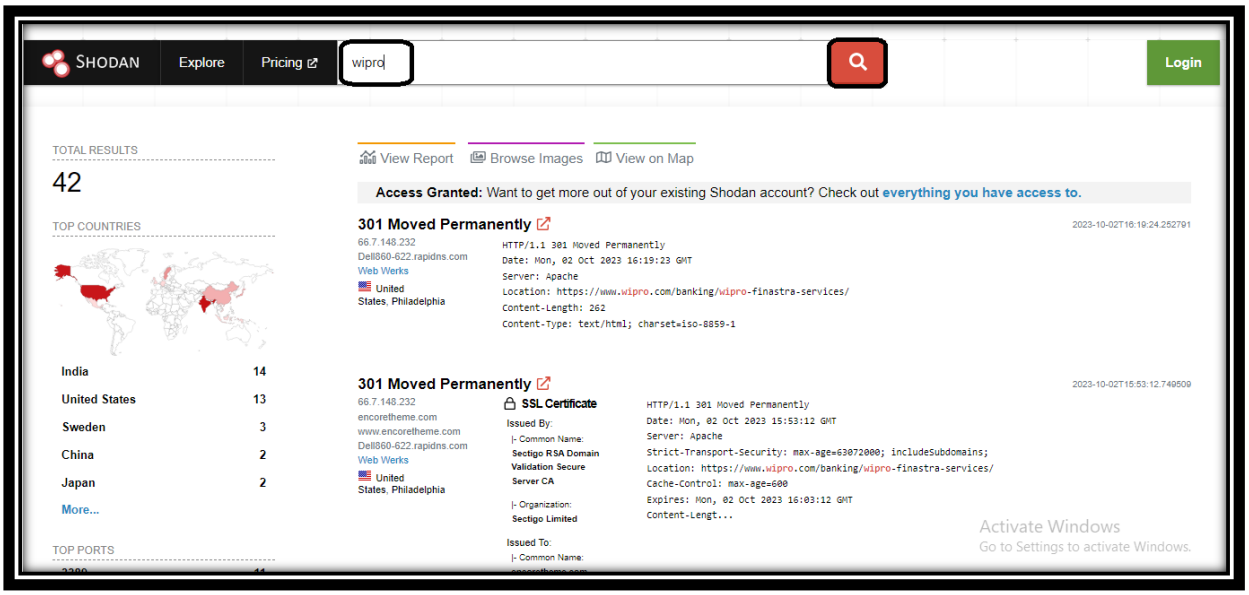
Gather information from IoT search engines

- 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

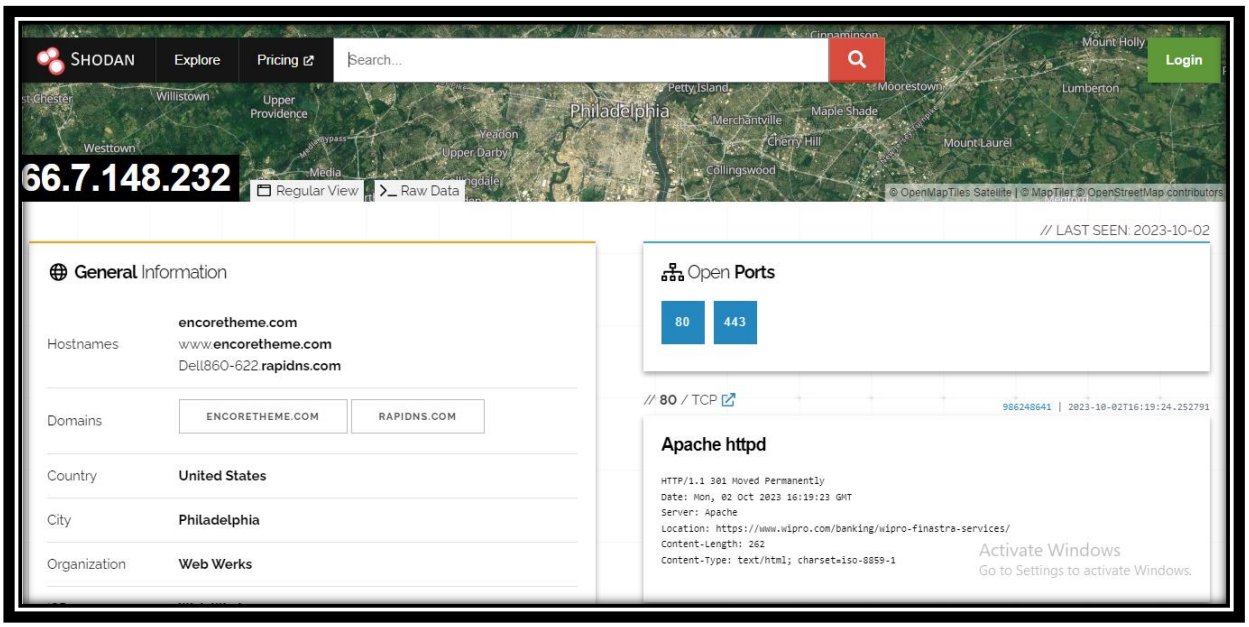
Target Organization: **WIPRO**
IoT Search Engine: **SHODAN (shodan.io)**

1. I started by opening my browser and navigating to Shodan.io.
2. Once on Shodan's platform, I entered my target into the search bar.
3. The search results provided me with various vulnerable details about my target, including server information, open ports, operating system, domains and more.





Then I navigated to the first result and got below information



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

Submitted By

Marepalli Rakesh

(Marepalli.rakesh@gmail.com)