Mini project -1

Footprinting

Submitted by - Aditi Devi Prasad

Batch - August 2024

Date – 25/11/2024

Footprinting is a process of gathering vulnerabilities to find the probable strategy of attacks using third-party sources. This process is not malicious. Based on the information collected from third-party sources, we segregate the possible vulnerabilities across the target.

- Footprinting is used to perform accurate attacks.
- It is an easy process as it involves only collecting the information.
- It is time saving because we know our target and the roadmap to achieve the same.

Footprinting process can be performed well by,

1. Basic steps
2. Advanced steps

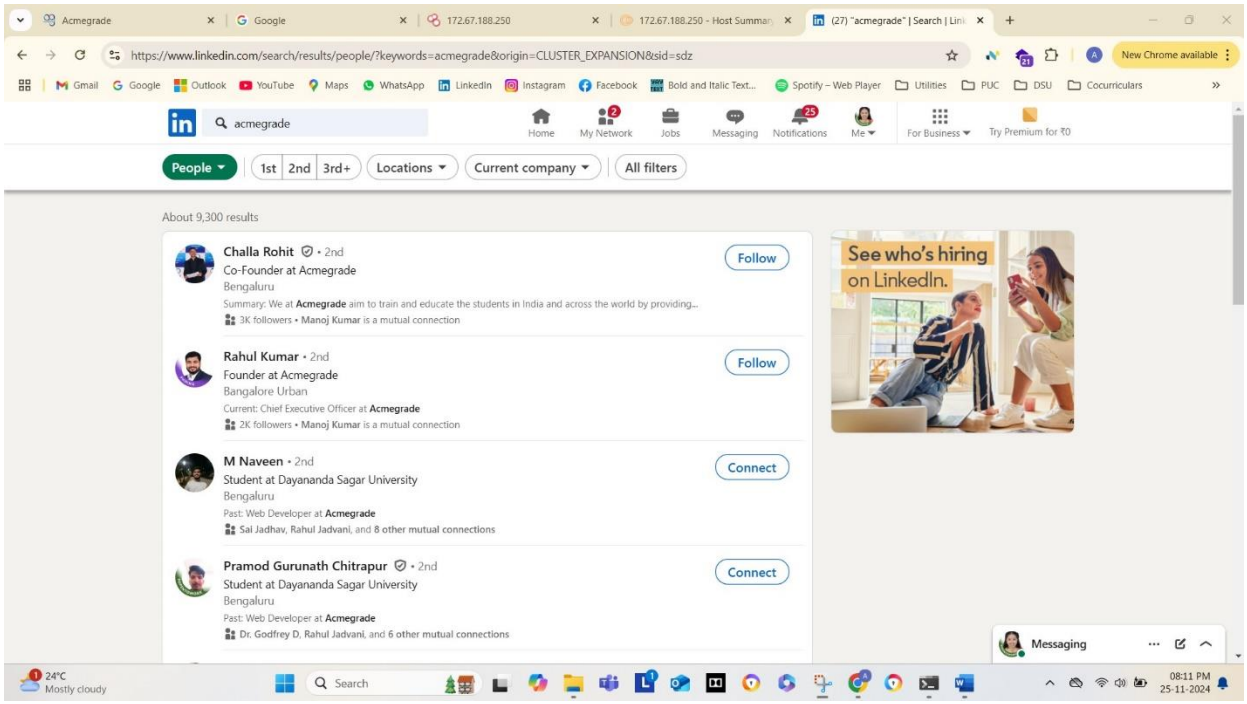
The website chosen for footprinting is www.acmegrade.com.

There are three basic steps in footprinting.

1. Footprinting using social networking websites.
   Trying to find possible candidates who can be vulnerable for hacking. By finding out the candidates in different social media with similar naming conventions, titles in blogs, titles against pictures etcetera gives us hints on the patterns individuals commonly use. For example, if there is a person named Anil_0902 across all three social media platform, possibility of Anil using same password across all platforms and possibly 0902 indicating some key date like birthday, anniversary etcetera.

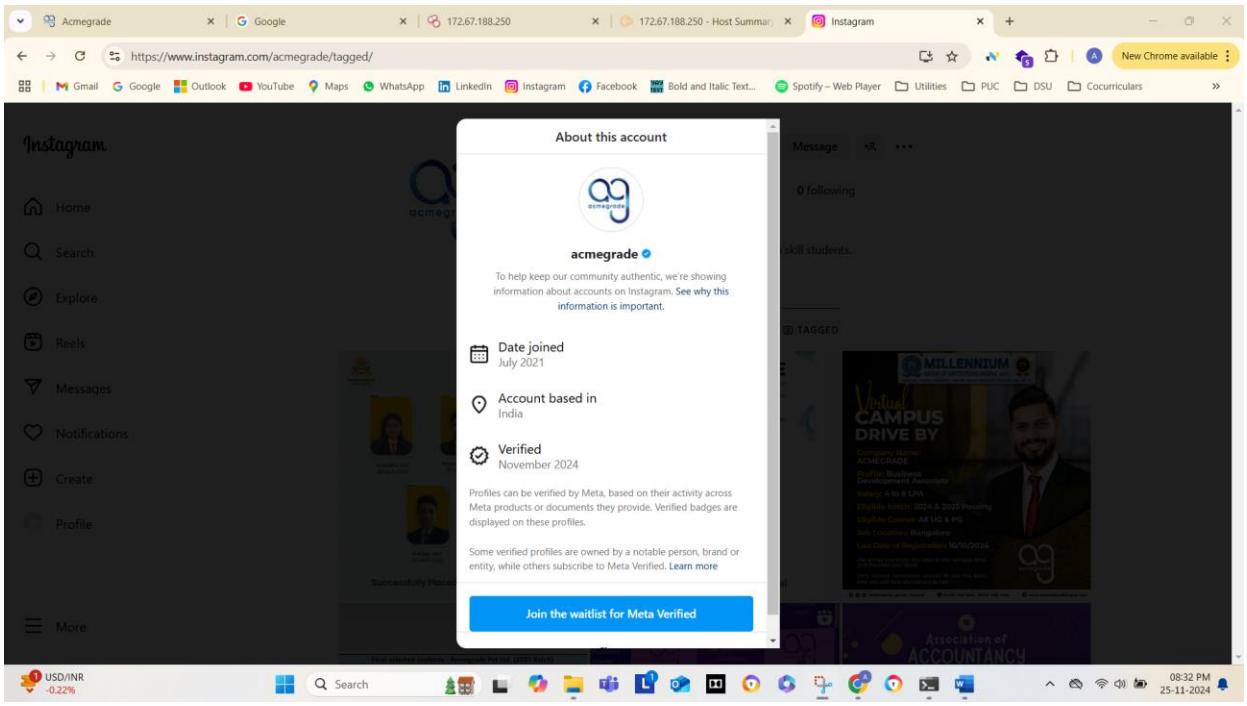
   These profiling will be helpful for hacking in future.

   a. LinkedIn:
      - There are 9300 alumni from acmegrade.
      - There are three jobs available since past 2 weeks.
      - Recent post is posted before 1 day.
      - It has 1 group within it.
      - 292 services are provided from acmegrade.
      - No events, courses present in this media.
      - It is an educational organisation situated mainly in Bengaluru North, Karnataka.
      - It has 26K followers and around 201-500 employees.



b. Instagram:

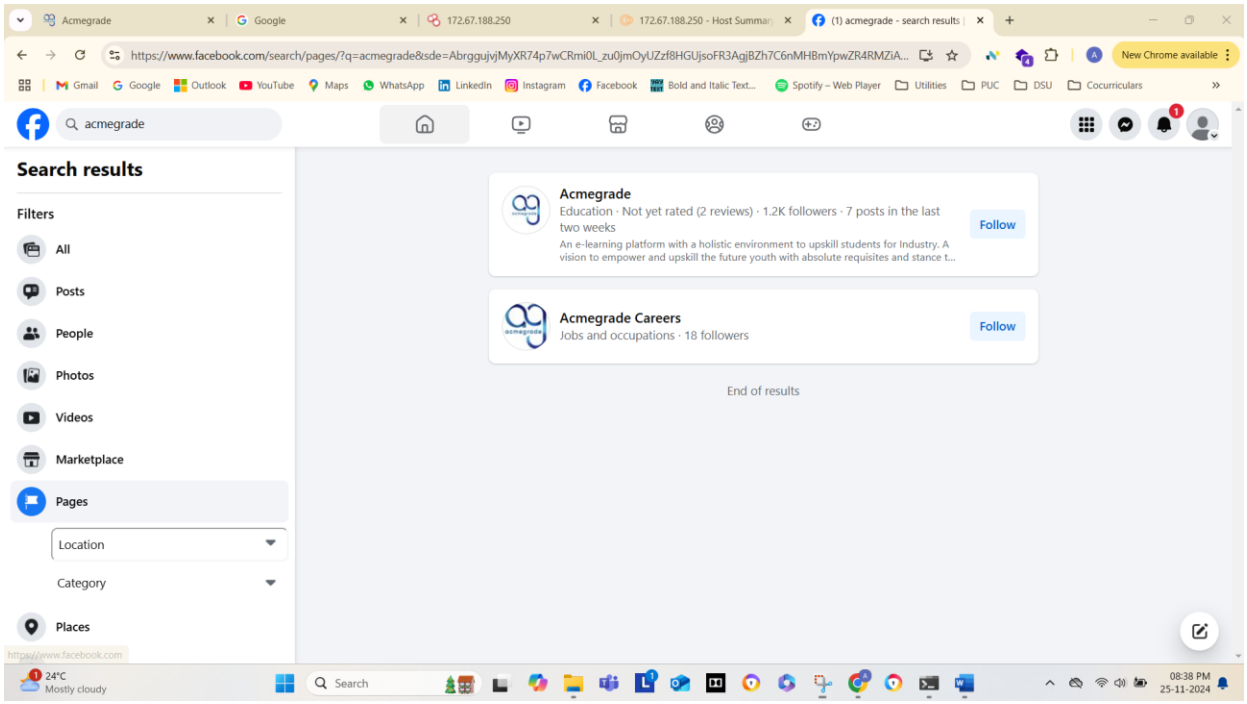
- There are 308 posts.
- 6775 followers are present.
- Acmegrade is not following anyone.
- E-learning platform link is provided.
- They joined Instagram on July 2021.
- This account is verified on November 2024.
- This educational company is based in India.



c. Facebook:

- 7 posts are posted in last two weeks.
- It has only 2 reviews and not yet rated.

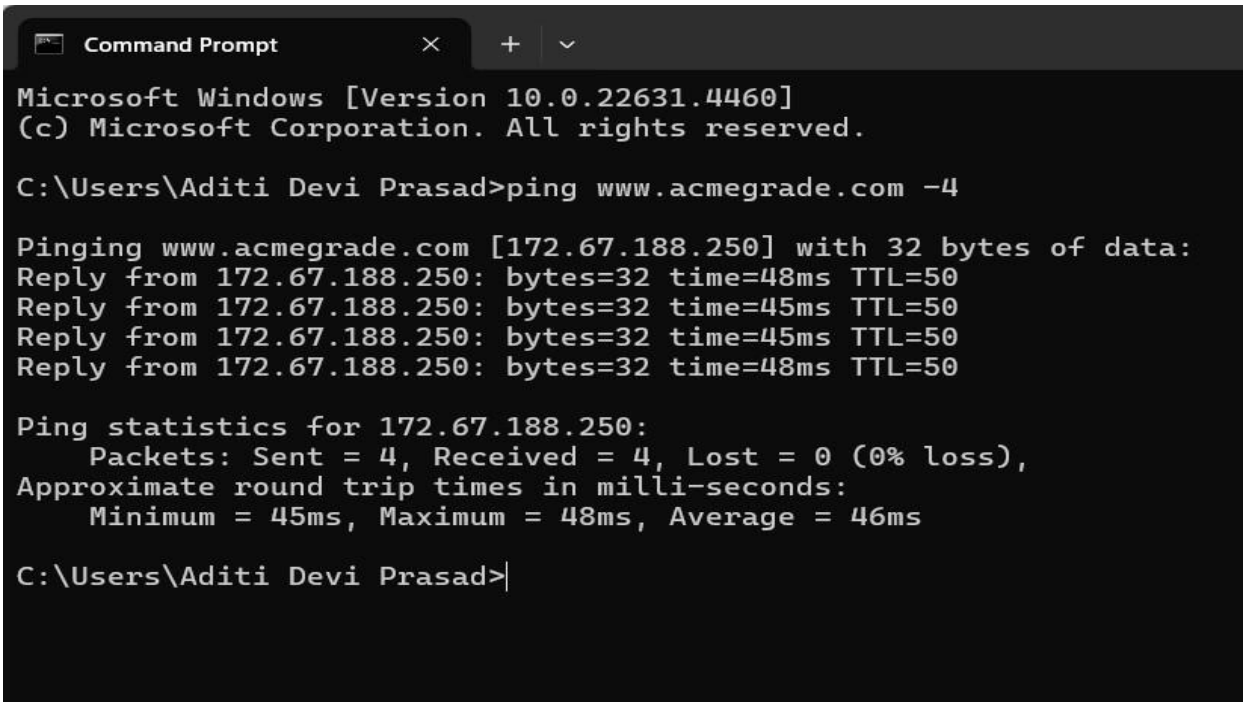
- Acmegrade careers account is dedicated for Jobs and occupations.
- There are 18 followers for Acmegrade careers account.
- There are 1.2K followers in main account.
- WhatsApp contact information is also given.



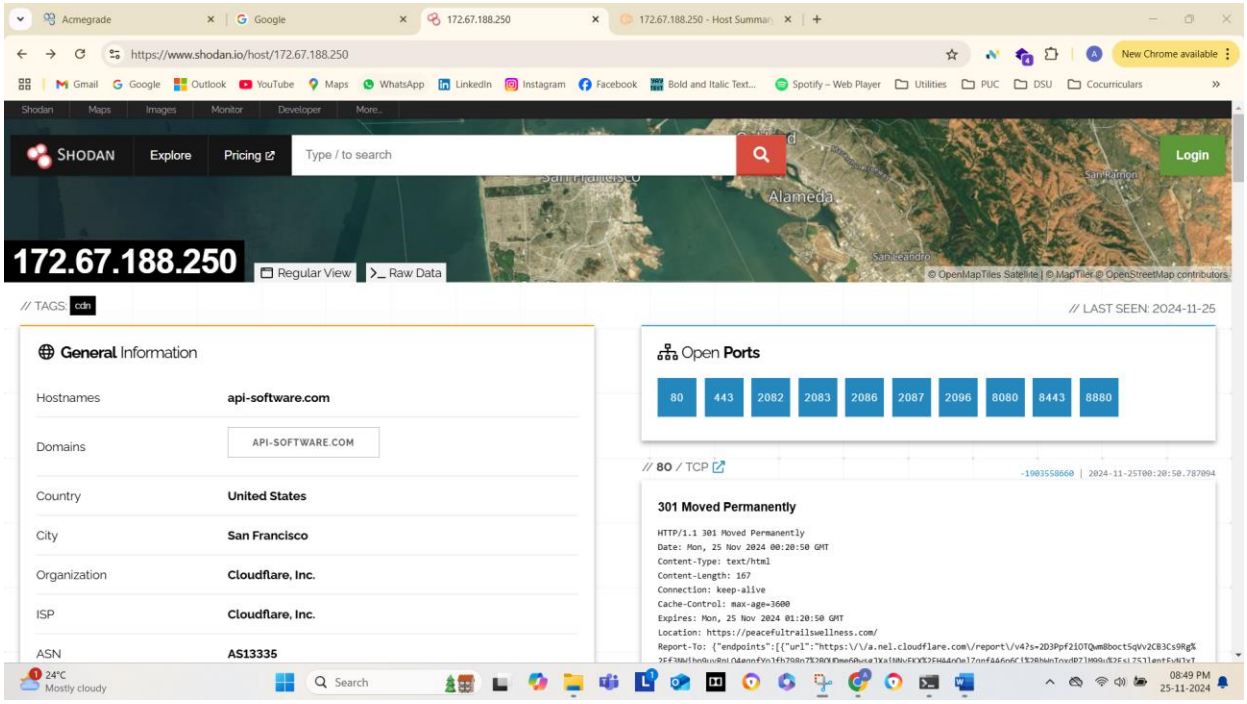
2. Use hacking search engine

Through hacking search engine, we can further collaborate possible methods, devices which are prone with vulnerabilities can be utilized for hacking. This is second logical step in hacking after individual profiling. Now we can easily connect these vulnerable devices with vulnerable individuals from point 1.

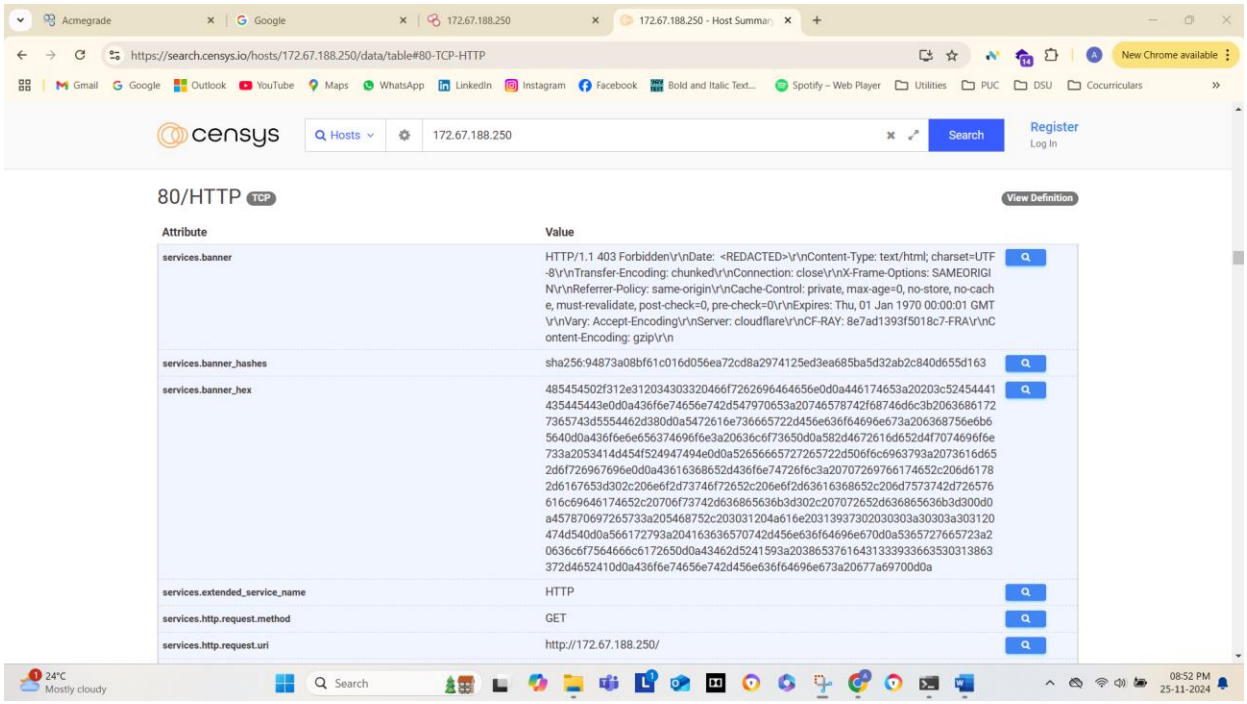
IPV4 address is found by using command prompt.



- Open ports available are 80, 443, 2082, 2083, 2086, 2087, 2096, 8 080, 8443, 8880.
- **api-software.com** is its domain as well as hostname.
- Its ASN number is [AS13335](AS13335).
- It is secured using Cloudflare, Inc. technology.
- HTTP/3 is the web technology used.
- Direct IP access not allowed.
- 400 The plain HTTP request was sent to HTTPS port.

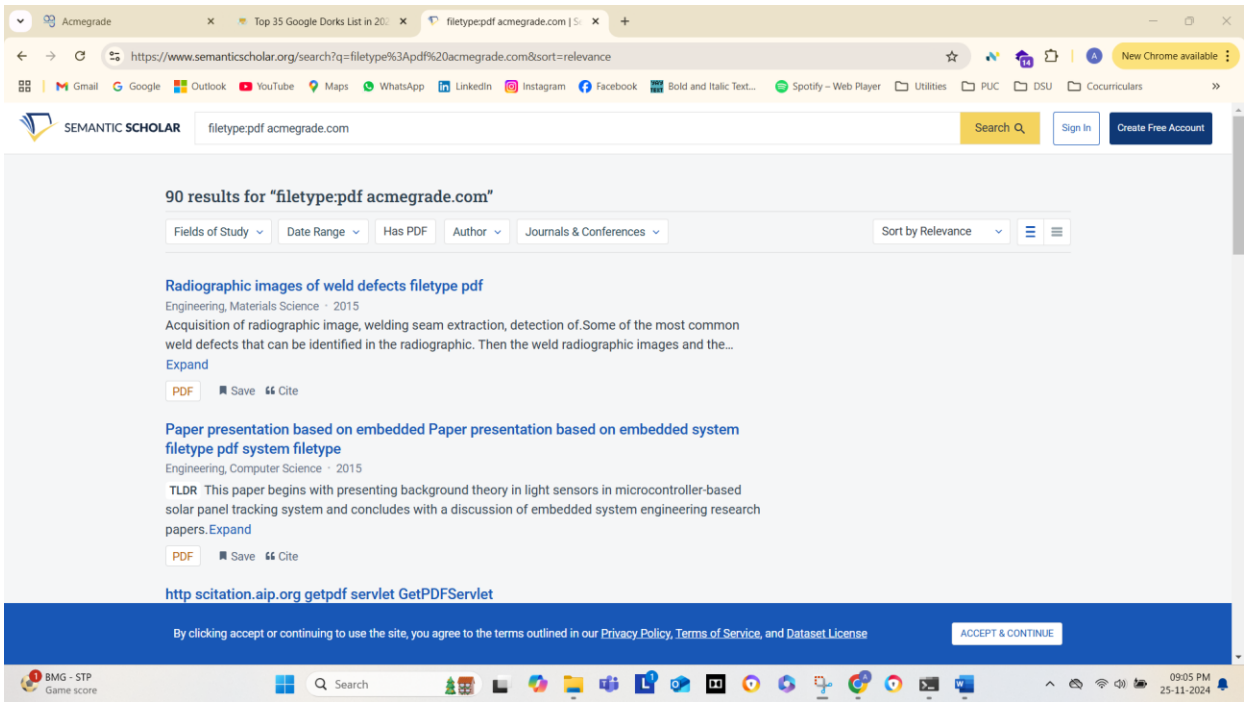


- 13 services are provided.
- syibayt.com, www.wplogify.com, realios.com, mail.arampolyfoam.com are some of the forward DNS.
- CloudFlare Load Balancer is the software used.



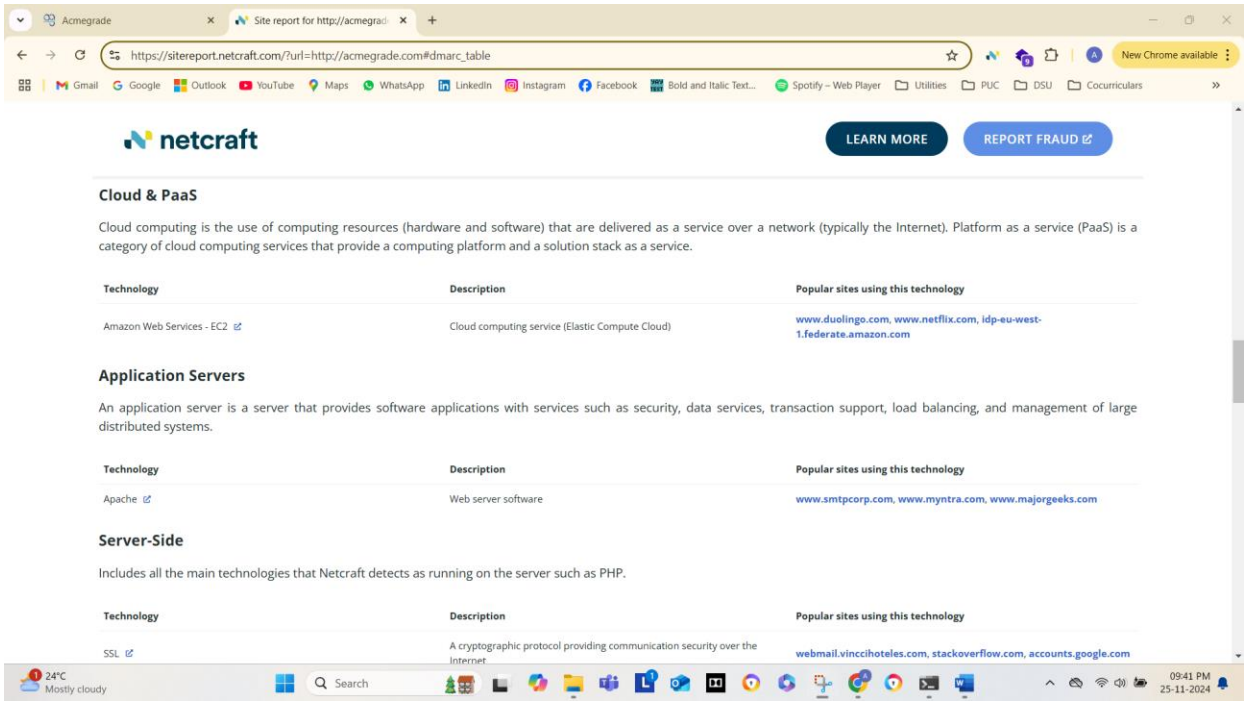
3. By using advanced search components of google.
   Now that we know the possible devices and possible individuals who can be used for our hacking, in this step we will further progress in trying to identify the further means/mode of attacking. Here we try to find whether the attack can be executed using excel, pdf, doc, URL, SQL injection.

   - intitle – no pages found.
   - filetype – 90 pdfs are found.
   - inurl – 3 results are found.
   - filetype – 2 text documents are found.
   - No papers found for admin/login
   - No open git repositories found.

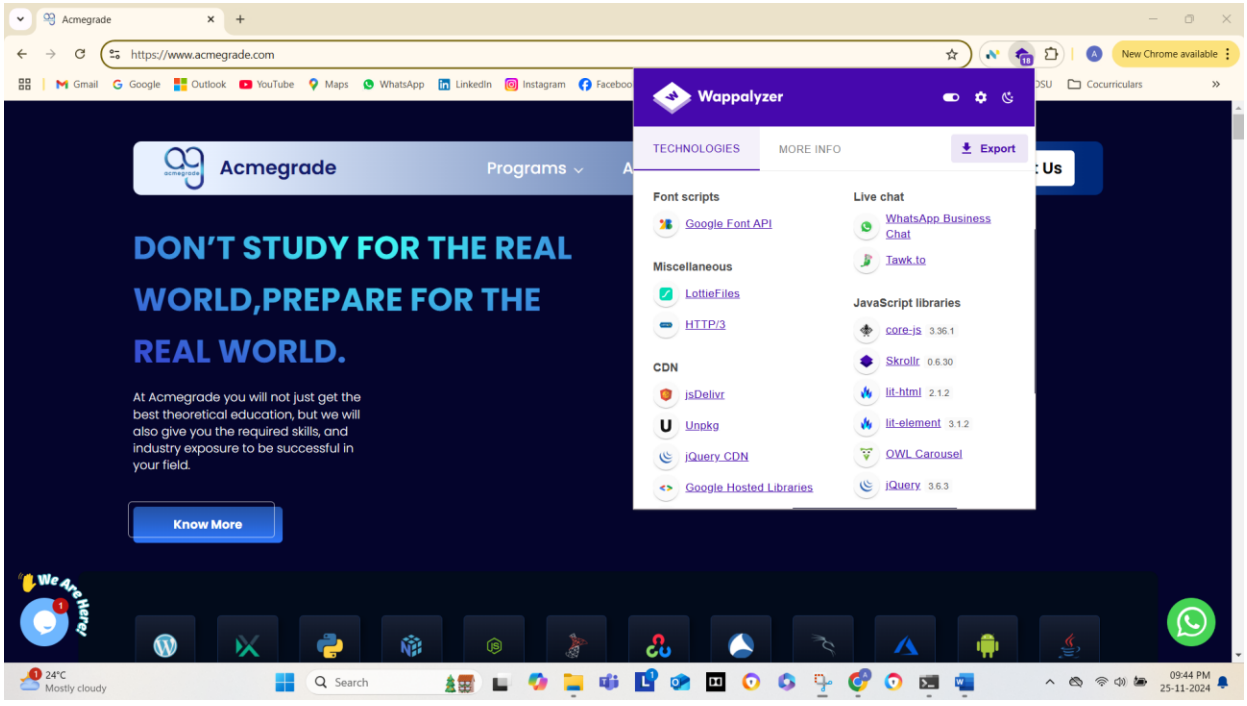


Let us now look into the advanced steps of footprinting.

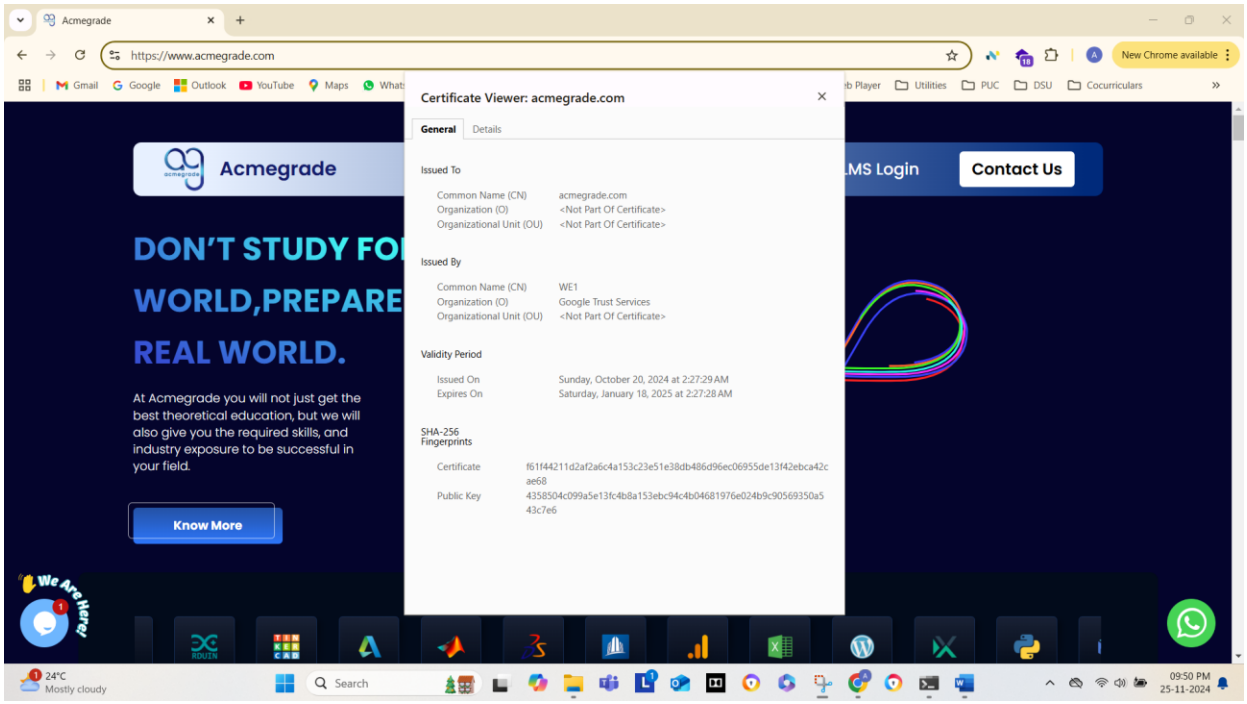
1. More details about the technologies used across a website.
   To find out vulnerabilities in each technology we use this.
   a. Using Netcraft extension:
      - This website is first seen on October 2021.
      - Title found is Acmegrade.
      - Hosting company is Cloudflare.
      - Hosting country is US.
      - IPV4 address is 104.21.49.49
      - Reverse DNS is unknown.
      - Name server is gracie.ns.cloudflare.com
      - DNS security extensions are enabled.
      - There are four IPV4 ranges.
      - There are four IPV6 ranges.
      - This host does not have a DMARC record.
      - 4 known web trackers were identified which were Cloudflare, Google, jQuery, jsDelivr.



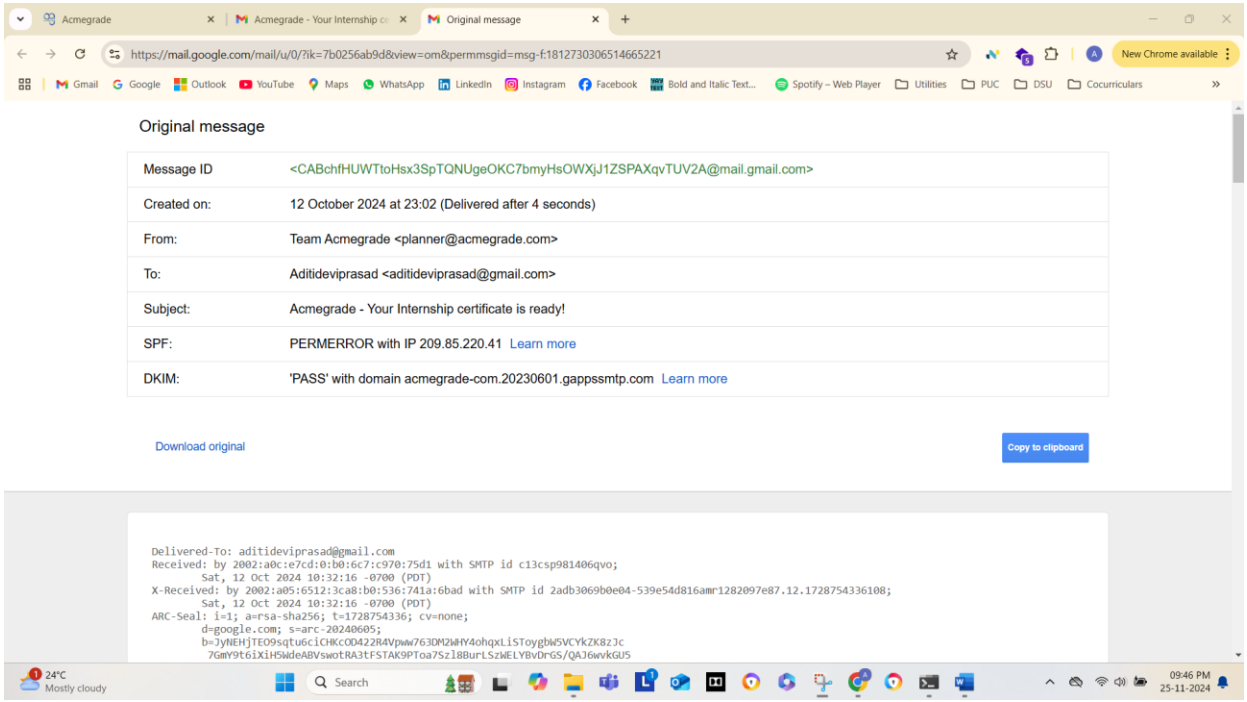
b. Using Wappalyzer extension:
   - One font script is used.
   - 2 miscellaneous technologies are used.
   - 2 live chats are used.
   - Many JavaScript libraries are used.



c. Identification of secured connection of website:
   - The connection is secure and it has the certificate for it.
   - Organization and it's unit is not a part of certificate.
   - It has a common name.
   - Validity period is from October 2024 to January 2025.



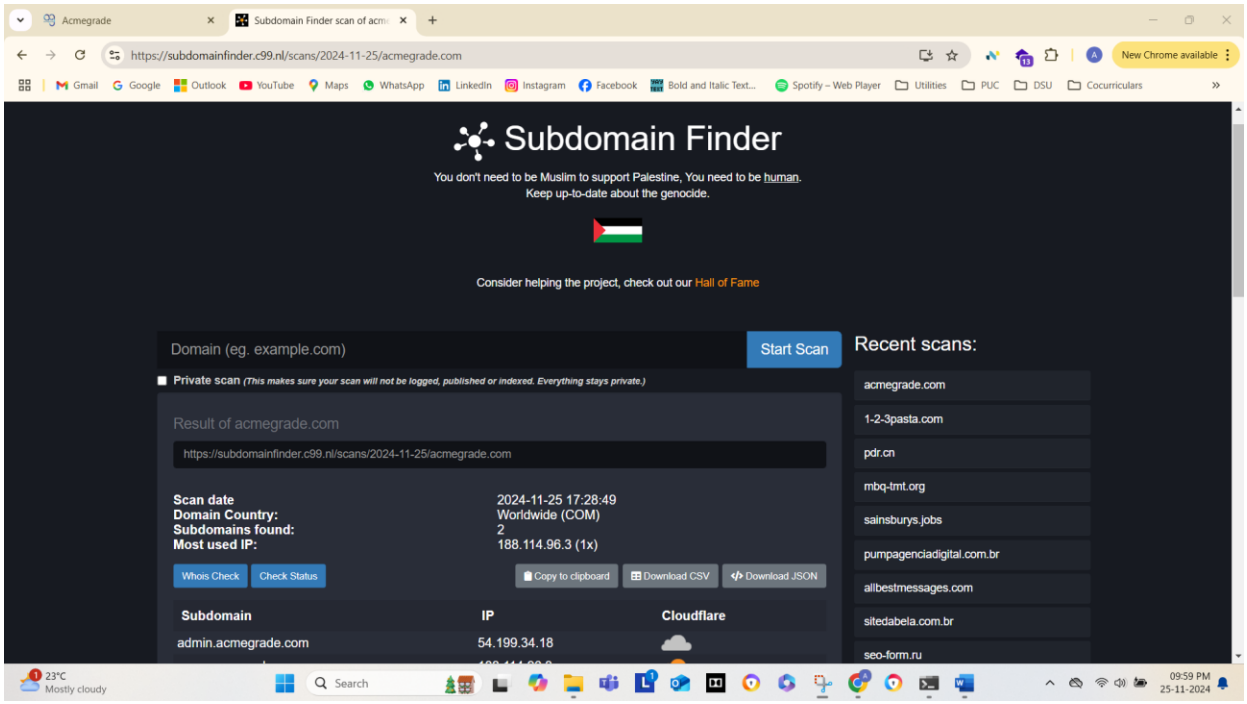
d. Verifying email validity:
   - SPF – it has PERMERROR.
   - DKIM – the test is passed.



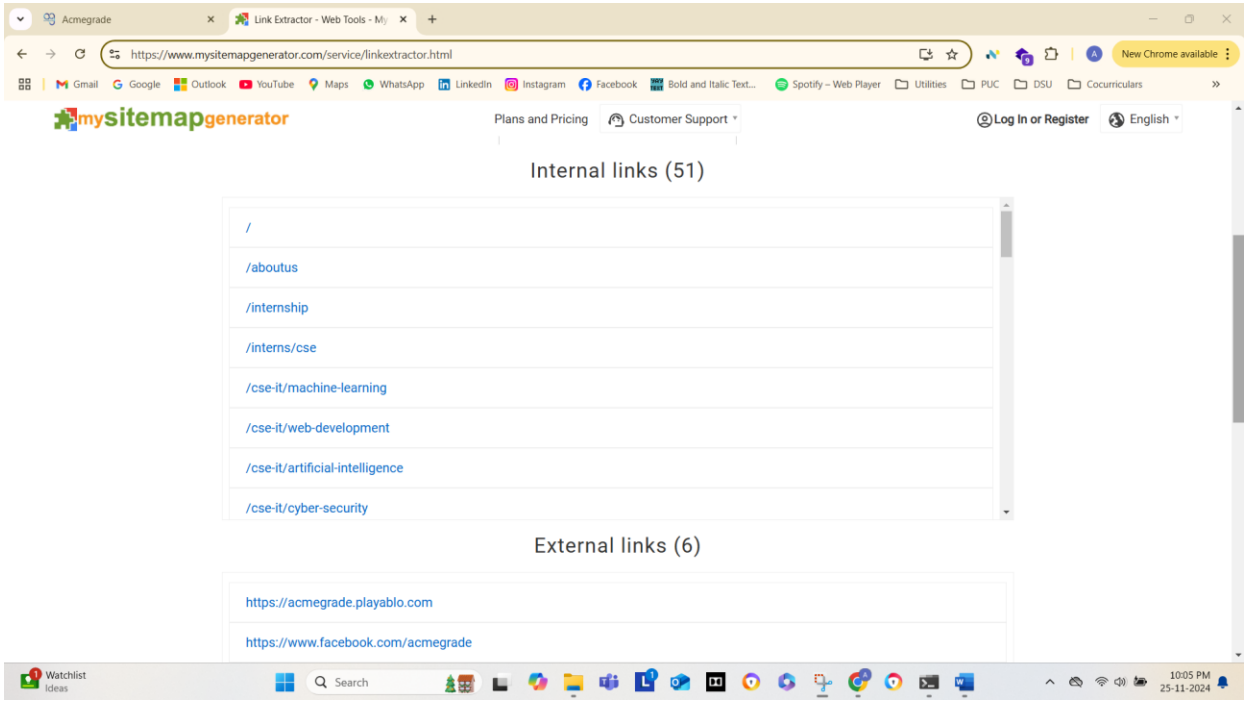
2. Find the sub-domains of a website

We get to know the network segmentation and possible additional effort needed for east-west movement.

- There are two subdomains found.
- Domain country is worldwide.
- The last scan of this domain was on March 2024.
- IP count is 1.
- Cloudflare is on for only one website.



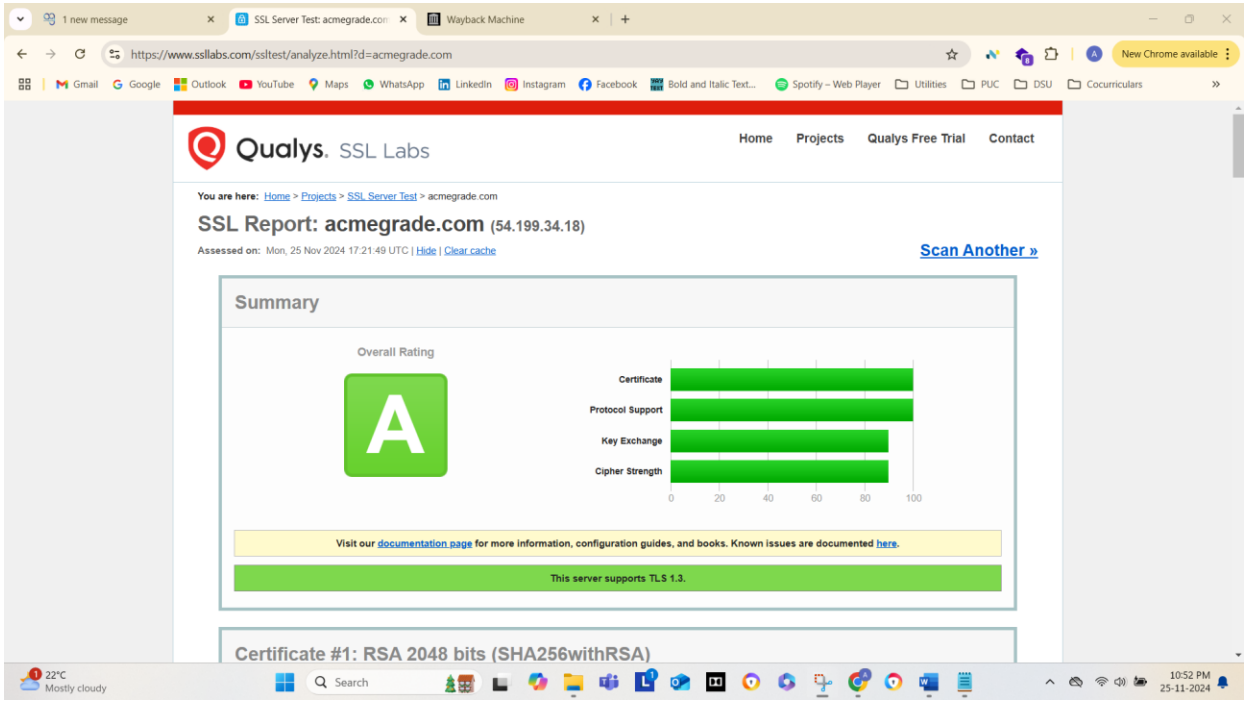
3. Find all the URLs of a site
   We find possible entry points here.
   - There are 57 URLs in total.
   - 51 URLs are internal links.
   - 6 URLs are external links.
   - All 57 links are Dofollow links.
   - There are zero Nofollow links.



4. Find Buffer size of a website
   Trying to get further data for loopholes.
   - The maximum buffer size identified is 1472bytes.

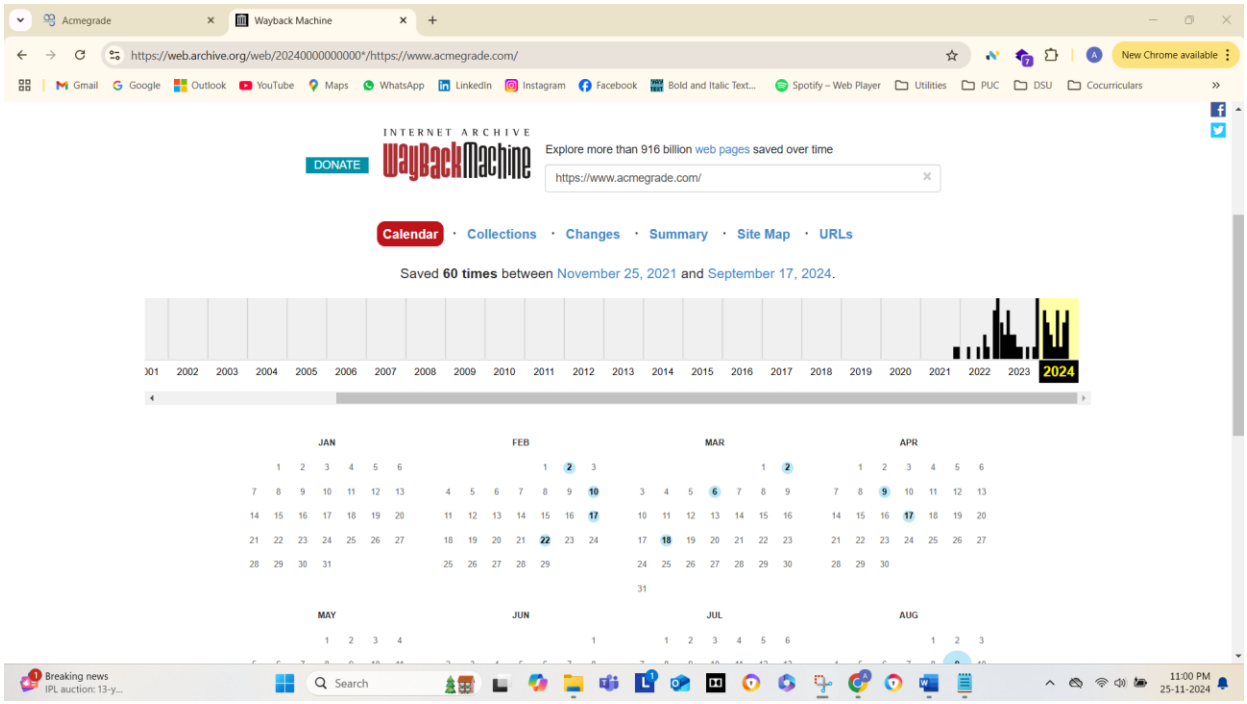
```
Command Prompt
Packet needs to be fragmented but DF set.

Ping statistics for 172.67.188.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Aditi Devi Prasad>ping -f -l 1472 172.67.188.25

Pinging 172.67.188.25 with 1472 bytes of data:
Reply from 172.67.188.25: bytes=1472 time=133ms TTL=49
Reply from 172.67.188.25: bytes=1472 time=177ms TTL=49
Reply from 172.67.188.25: bytes=1472 time=328ms TTL=49
Reply from 172.67.188.25: bytes=1472 time=198ms TTL=49

Ping statistics for 172.67.188.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 133ms, Maximum = 328ms, Average = 209ms

C:\Users\Aditi Devi Prasad>ping -f -l 1473 172.67.188.25

Pinging 172.67.188.25 with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 172.67.188.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Aditi Devi Prasad>
```

5. SSL/TLS testing
   Trying to find out what is the secure channel established which helps us in decoding it.
   - Overall rating is good.
   - Key used is RSA 2048 bits (e 65537).
   - There is no weak key.
   - Issuer is R11.
   - No chain issues found.
   - Signature algorithm is SHA256withRSA.
   - Only TLS 1.3 and TLS 1.2 protocols are used.
   - There are 5 handshake failures.



6. Time-travel on a website
   Trying to find the historical trends of the website.

- Saved 60 times from November 2021 to September 2024.
- 65.34% of the websites are images.
- Website drastically improved from 2021 to 2022.
- Last modified was in September 2024.



This completes all steps of footprinting.

Summary (Conclusion):

Footprinting technique had more sections which allowed to gather all precise information on the website which was useful to identify the vulnerability and hack into the machine. The few vulnerabilities identified are as follows.

- Open port 8080 which is using http protocol, can be vulnerable as compared to 8443/https combination.
- Animation downloads are allowed from LottieFiles which can be a vulnerability.
- There are two subdomains and one subdomain is not protected by CloudFlare technology which can be a major loophole to hack in.
- Organization and Its unit are not a part of secure connection certificate.