

# **MINI PROJECT -1**

## **ACMEGRADE Cyber Security (April'24)**

### **FOOTPRINTING**

Submitted by: R.Yogeshram

Email: [yogeshramr@gmail.com](mailto:yogeshramr@gmail.com)

# RECON-FOOTPRINTING

## What is Footprinting?

Footprinting is a technique used to gather information about a target's digital footprint, such as a computer system, network, or infrastructure, to identify potential vulnerabilities.

It involves collecting data over time, which can include scanning open ports, mapping network topologies, and using tools like ping sweeps or traceroute commands.

The goal is to build a broad profile of the target that can help determine how to successfully attack the system.

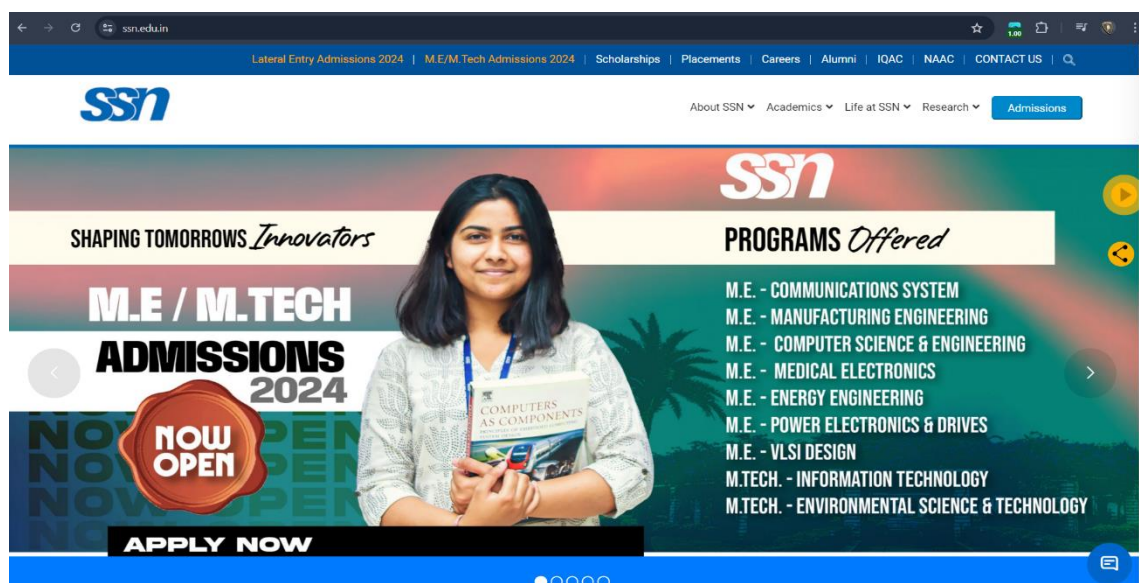
## Basics of Footprinting:

1. Using social networking sites (Facebook,insta,X)
2. Using hacking search engines (Shodan,Censys,not-evil, duck duck go)
3. Advanced google search commands (Google dork)

Target : SSN college of engineering

Note: The following are done in a closed environment and I executed with a pure intention of gathering recon w.r.t to my college website , everything is done for ethical and learning purposes.

College website: <https://www.ssn.edu.in/>



## STEP-i

### ❖ Using social networking sites:

To gather resources and intelligence on the target one of the best possible way is to look on social media/networking sites like Facebook , Instagram, X(twitter). By looking at such social sites we get to know what the institute is about and what are the courses offered and where the institute is located at . Although this Recon may seem very basic but is a crucial factor in getting to know what , when to expect while proceeding further.

While performing the following are the recon I was able to gather

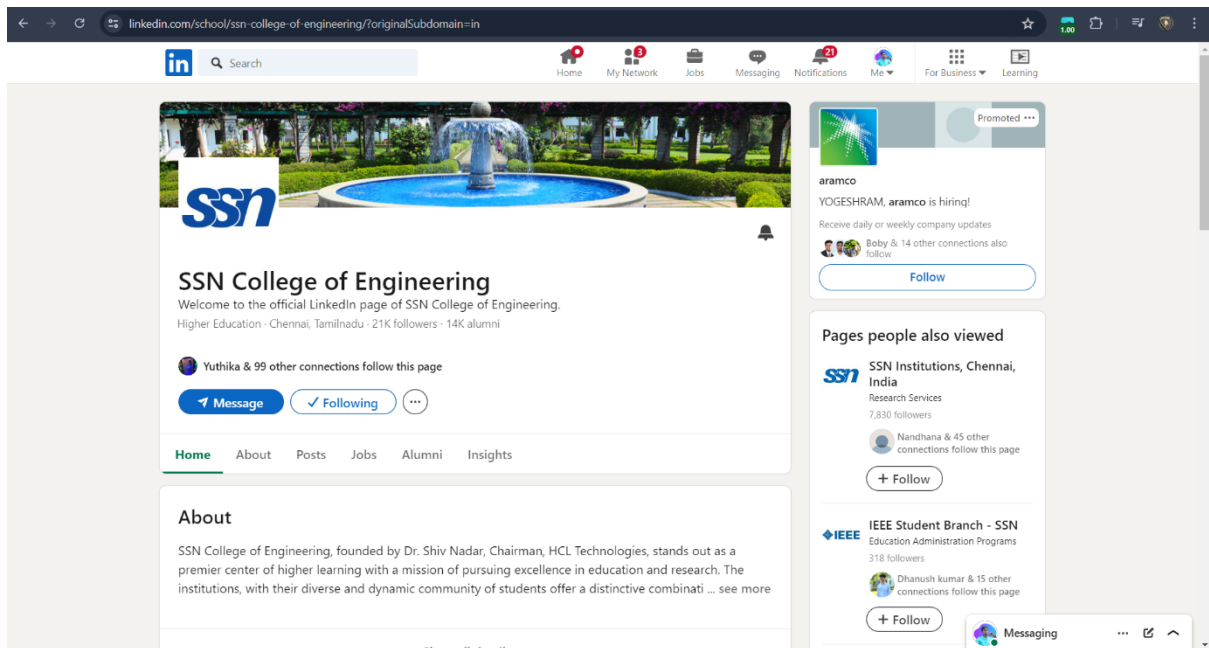
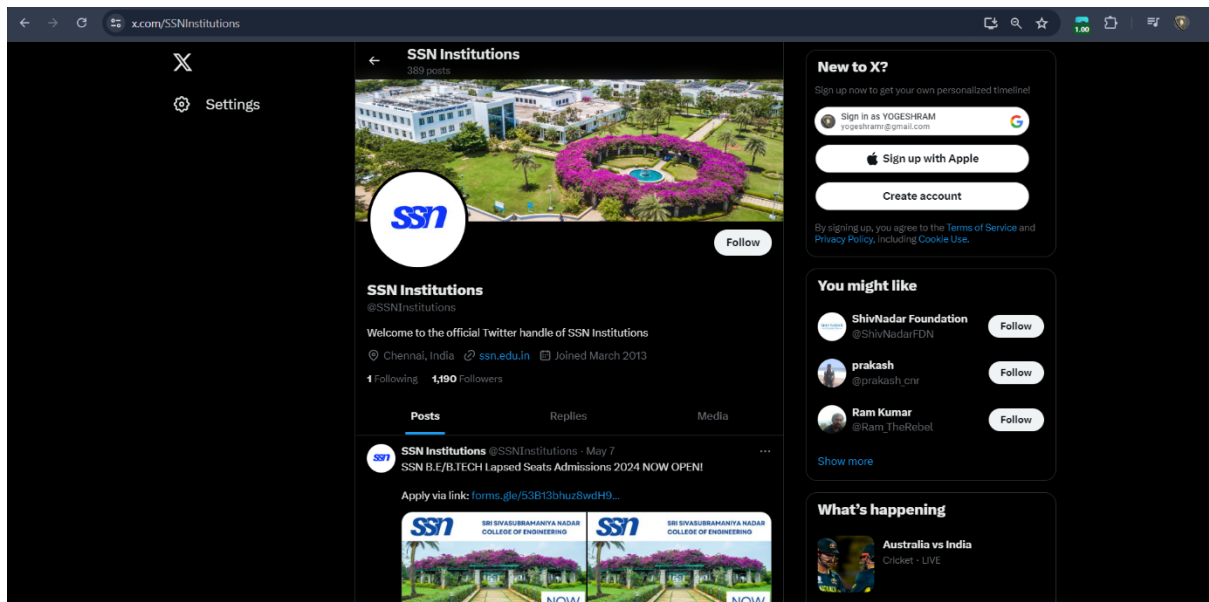
The image displays two screenshots of social media profiles for SSN Institutions.

**Instagram Profile:** The profile is for 'ssninstitutions' with 278 posts, 4,237 followers, and 18 following. The bio states: 'SSN Institutions Education. Welcome to the Official Instagram page of SSN Institutions. SSN Institutions offer programs in Engineering, Management,... more Kalavakkam, Old Mahabalipuram Road (OMR), Chennai, India 603110 @linktr.ee/ssn\_institutions'. Below the bio are four story highlights: 'Alumni speak', 'Admissions', 'Important', and 'SSN App'. The main feed shows a post for 'M.E./M.TECH ADMISSIONS 2024 IN-PERSON OPEN HOUSE' with a registration link.

**Facebook Profile:** The profile is for 'SSN - Institutions' with 9.2K likes and 9.4K followers. The bio states: 'SSN - Institutions is at SSN College of Engineering. Ready to take your academic journey to the next level? Lateral entry admissions are now open! Secure your spot and become a part SSN of SSN B.E/B.TECH Lateral Entry Admissions Apply via link in Bio #SSN #JoinUsNow #CollegeAdmissions'. The 'Intro' section provides contact information: 'Page · University', 'Kalavakkam, Old Mahabalipuram Road (OMR), Chennai, India, Tamil Nadu', '044 2746 9700', 'info@ssn.edu.in', and 'ssn.edu.in'. The main feed shows a post for 'B.E./B.TECH LATERAL ENTRY' with a registration link.

Log in or sign up for Facebook to connect with friends, family and people you know.

Log in or Create new account



From the above gather recon I was able to come to conclusion that SSN college of engineering is offering multiple courses and I was able to collect from more insight on the faculty list and list of events that are set to take place.

## Step-ii

### ❖ Using Hacking Search

First letz try to ping the college website using command prompt

```
C:\Users\ryoge>ping www.ssn.edu.in

Pinging www.ssn.edu.in.cdn.cloudflare.net [2606:4700:9c60:dc63:9cc6:c0b:ed0b:852] with 32 bytes of data:
Reply from 2606:4700:9c60:dc63:9cc6:c0b:ed0b:852: time=3ms
Reply from 2606:4700:9c60:dc63:9cc6:c0b:ed0b:852: time=5ms
Reply from 2606:4700:9c60:dc63:9cc6:c0b:ed0b:852: time=5ms
Reply from 2606:4700:9c60:dc63:9cc6:c0b:ed0b:852: time=5ms

Ping statistics for 2606:4700:9c60:dc63:9cc6:c0b:ed0b:852:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\Users\ryoge>ping www.ssn.edu.in -4

Pinging www.ssn.edu.in.cdn.cloudflare.net [104.18.8.214] with 32 bytes of data:
Reply from 104.18.8.214: bytes=32 time=6ms TTL=52
Reply from 104.18.8.214: bytes=32 time=6ms TTL=52
Reply from 104.18.8.214: bytes=32 time=5ms TTL=52
Reply from 104.18.8.214: bytes=32 time=6ms TTL=52

Ping statistics for 104.18.8.214:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

From the above image we can see that we are able to ping and get response from [WWW.ssn.edu.in](http://WWW.ssn.edu.in)

The screenshot shows the AbuseIPDB website interface. At the top, there's a navigation bar with links like Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, and Contact. Below this, the main heading reads "AbuseIPDB » 104.18.8.214". A search bar at the top of the main content area contains the IP address "2405:201:e045:506a:edb2:13a:4b1c:4402" with a "CHECK" button. Below the search bar, a message states "104.18.8.214 was not found in our database". A table provides details for the IP: ISP (CloudFlare Inc.), Usage Type (Content Delivery Network), Domain Name (cloudflare.com), Country (United States of America), and City (San Francisco, California). At the bottom of the table, there's a note: "IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly." Below the table, there are two buttons: "REPORT 104.18.8.214" and "WHOIS 104.18.8.214".

Using “Shodan” to obtain more details and information on the target

The screenshot shows the Shodan web interface in a browser. The address bar displays 'shodan.io/host/104.18.9.214'. The page features a dark theme with a navigation bar at the top containing 'Shodan', 'Maps', 'Images', 'Monitor', 'Developer', and 'More...'. Below the navigation bar, there's a search bar with 'SHODAN' and 'Explore' buttons, and a 'Login' button. The main content area displays the IP address '104.18.9.214' in a large font, with 'Regular View' and 'Raw Data' tabs. To the left, under the heading 'General Information', there's a table with the following data:

Country	United States
City	San Francisco
Organization	Cloudflare, Inc.
ISP	Cloudflare, Inc.
ASN	AS13335

To the right, under the heading 'Open Ports', there's a list of ports: 80, 443, 2082, 2083, 2086, 2087, 2096, 8080, 8443, and 8888. Below this, the selected port '80 / TCP' is shown with a status of 'Direct IP access not allowed | Cloudflare'. The raw data for port 80 is displayed, showing an HTTP 403 Forbidden response with various headers and a timestamp of '2024-06-22T11:06:12.418893'.

From Shodan I was able to analyze the following web technologies

Advertising: Linedin Ads

CMS (Content Management System): Adobe experience manager

Cookie Compliance: OneTrust

JavaScript Libraries: jQuery

Programming Languages: Java

Video Players: YouTube

Open ports:

PORT 80

PORT 2087

PORT 443

PORT 2096

PORT 2082

PORT 8080

PORT 2083

PORT 8443

PORT 2086

PORT 8888

Using “Censys” (search.censys.io) to obtain further more info.

The screenshot displays the Censys search results for the IP address 104.18.9.214. The interface includes a search bar at the top with the IP entered. Below the search bar, the IP is listed with a timestamp: "As of: Jun 27, 2024 12:52pm UTC | Latest". The main content area is divided into sections: "Basic Information" and "HTTP 80/TCP".

**Basic Information:**

- Forward DNS:** telener-360.lapieza.io, yo-dispongo.lapieza.io, feriavirtual.lapieza.io, consultores-avanzados-de-vida-sc.lapieza.io, saigonvn.net, ...
- Routing:** 104.18.0.0/20 via CLOUDFLARENET, US (AS13335)
- Services (13):** 80/HTTP, 443/HTTP, 2052/HTTP, 2053/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2095/HTTP, 2096/HTTP, 8080/HTTP, 8443/HTTP, 8880/HTTP

**HTTP 80/TCP:** 06/26/2024 20:55 UTC

**Software:** CloudFlare Load Balancer

**Details:**

- http://104.18.9.214/**
- Status:** 403 Forbidden
- Body Hash:** sha1:d2e86f8c1fb6a0162ae8bbf2a66a59f9eb5ea36
- HTML Title:** Direct IP access not allowed | CloudFlare
- Response Body:** [EXPAND]

**Geographic Location:**

- City:** San Francisco
- State:** California
- Country:** United States (US)
- Coordinates:** 37.7621, -122.3971
- Timezone:** America/Los\_Angeles

the summary provide by censys was much better to analyse and it had detailed description of the each port with the following parameters Status, Body hash, HTML Title & Response body

### Step-iii

❖ Advanced google search components (Google Dork)

#### What is Google Dork ?

Google dorks, also known as Google hacks, are search queries that use advanced operators to find information that may not be available through standard Google searches. Google dorks can be used for a variety of purposes.

Searching for specific information:

We can use Google dorks to find key phrases or topics on specific websites, find specific file types, or look for certain keywords in a web page's title.

Finding sensitive information:

Google dorks can help us identify potential security risks or sensitive information that may be unintentionally exposed on websites. For example, a



hacker could use a Google dork to find and exploit SSH private keys to decrypt sensitive information.

The screenshot shows a web browser displaying a "Google Dorks Cheat Sheet" from stationx.net. The page has a dark theme and a sidebar with a "Table of Contents" and a "Level Up in Cyber Security" banner. The main content area is a table with two columns: "EXAMPLES" and "DESCRIPTION".

EXAMPLES	DESCRIPTION
<code>inurl:"view.shtml" "Network Camera"</code> <code>"Camera Live Image" inurl:"guestimage.html"</code> <code>intitle:"webcamXP 5"</code>	Get web applications showing live webcam (online camera) footage.
<code>"Not for Public Release" + "Confidential"</code> <code>ext:pdf   ext:doc   ext:xlsx</code>	Get links to documents meant to be classified. Some come from governmental websites.
<code>site:.hk &amp; inurl:wp-login</code>	Get login pages of WordPress sites ending in the notoriously <b>unsafe domain</b> ".hk"
<code>"index of" inurl:ftp secret</code>	Get FTP servers you want to access containing the keyword "secret"
Critical dorks performed on .env files yielding results such as: <code>Max@osca osca.munda.org: cawemo: .env  </code> <code>https://docs.osamunda.org/cawemo/1.5/.env</code> <code>... DATABASE # ***** DB_HOST="postgresql your company.com DB_PORT=5432</code> <code>DB_NAME=cawemo DB_USER=cawemo DB_PASSWORD=top secret 123 ***** #</code> <code>http://siatfor.ru: .env  </code> <code>siatfor.ru/.env</code> <code>... DB_PORT=3306 DB_DATABASE=waitefor_db DB_USERNAME=waitefor_db</code> <code>DB_PASSWORD=97huu123_0Y BROADCAST_DRIVER=ing CACHE_DRIVER=Me</code>	Popular web development frameworks use .env files to declare general variables and configurations for local and online dev environments, often including passwords. The dork used to produce the screenshot exposes database passwords. Hence it's vital to keep .env files from being publicly accessible. (If you've read this cheat sheet in its entirety, you will be able to guess the dork used here.)

Below the table, a note states: "This often-updated exploit database contains other Google dorks that expose sensitive information. Proceed with caution."

By using the following command (`filetype pdf ssn.edu.in`) in search bar of the search engine. we can curate the file type, by mentioning the file type we are looking for followed by the website or domain name

In this I was trying to obtain PDF format files from ssn.edu.in website

The screenshot shows a Google search results page for the query "filetype pdf ssn.edu.in". The search bar at the top shows the query. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Shopping", "Books", "Web", and "More". The search results are listed below, showing several PDF files from SSN Institutions.

Search results for "filetype pdf ssn.edu.in":

- SSN Institutions**  
https://www.ssn.edu.in/5001\_CSE\_R2021 | PDF |  
**Curriculum and Syllabus B.E Computer Science and ...**  
PROGRAM OUTCOMES (POs): On successful completion of the program, our graduates will be able to: 1. Engineering knowledge: Apply the knowledge of mathematics ...  
229 pages
- SSN Institutions**  
https://www.ssn.edu.in/ |  
**SSN Institutions**  
Programs at SSN Chennai are holistic, covering research, sports, entrepreneurship and much more, preparing students for the challenges of tomorrow.  
SSN SACE - The journey of ssn - Clubs at SSN - Why Choose SSN  
Missing: filetype | Show results with: filetype
- SSN Institutions**  
https://www.ssn.edu.in/uploads/2023/06/Mte... | PDF |  
**M.TECH**  
WHY STUDY AI & ML? Information technology. STUDY AMIDST LUSH GREENERY. IN SSN.  
JOIN US TO. NUTURE YOUR DREAMS.  
2 pages
- SSN Institutions**  
https://www.ssn.edu.in/... |  
**pdf - SSN Institutions**  
With their diverse and dynamic community of students, SSN offer a distinctive combination of



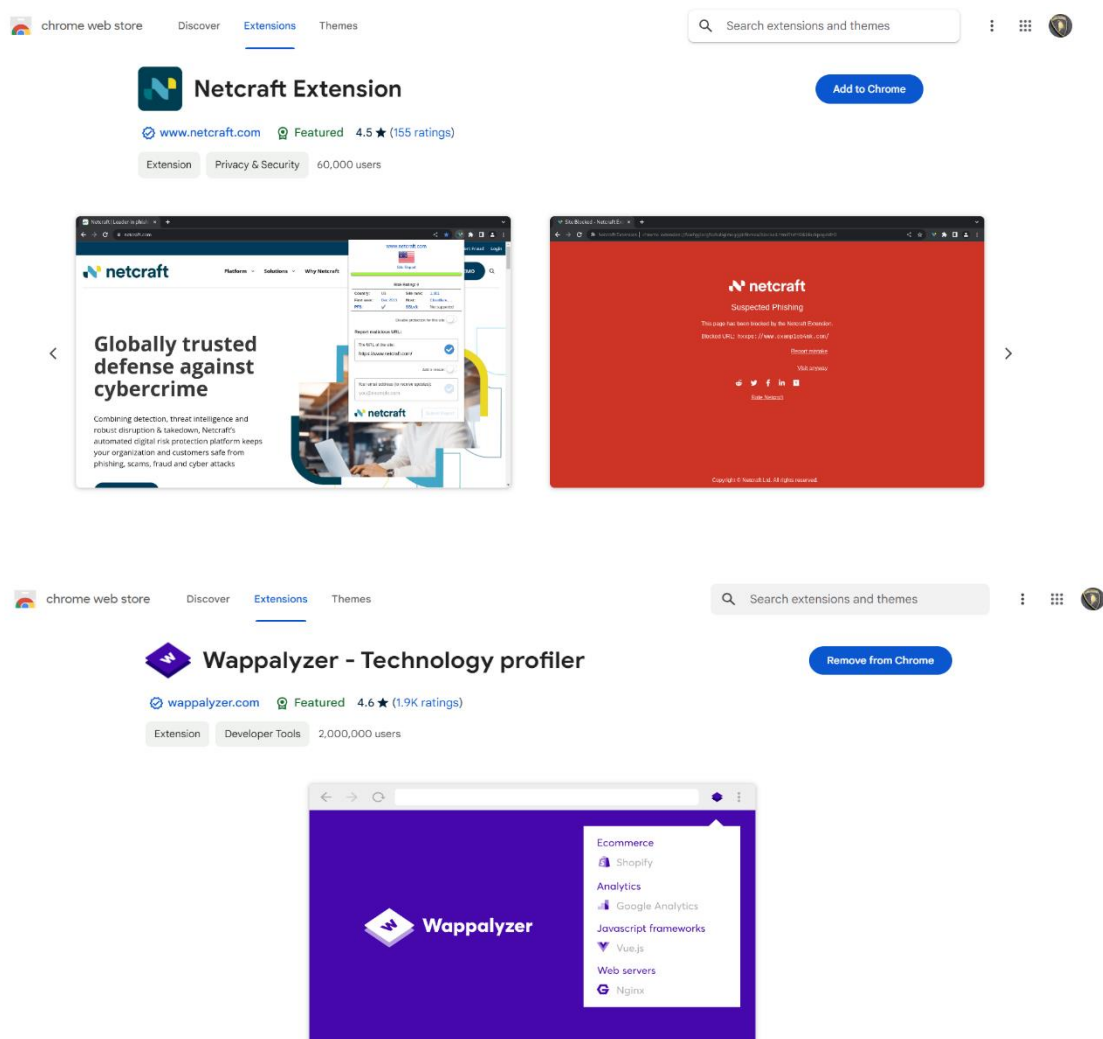
## Advanced Footprinting:

1. Knowing the website Technologies
2. Knowing subdomains of a website
3. Find all URL's on the website
4. Finding Security headers of a website
5. SSL / TLS test
6. Time travel across a website
7. Finding the Buffer size of a website

### Step i

❖ Knowing the website technologies.

This can be done with the help of chrome extensions “Netcraft” & “Wappalyzer”



## **What is Netcraft?**

The Netcraft Extension provides comprehensive site information and cybercrime protection when browsing the web. Users can also use the extension to report URLs they believe to be malicious to Netcraft.

## **How does the risk rating work ?**

The Risk Rating displayed by the Netcraft Extension offers a further level of protection against new sites that are not yet in Netcraft's database. A lower risk rating is better as it indicates lower risk. Although some sites contain entirely benign content, the Netcraft Extension may assign a high Risk Rating because it could be hosted under a newly registered domain, the site may have never been seen in the Netcraft Web Server Survey before, or the network hosting the site may have hosted a number of fraud sites in the past. Many other factors are also taken into account. Hosting a website on an unusual port number will also increase the Risk Rating, as will hosting a site from a raw IP address, as many phishing sites employ this tactic. The Risk Rating can be calculated fast enough to be performed for arbitrary sites as people visit them, and does not rely on manual categorization.

## **What is Wapplyzer ?**

Wappalyzer is a technology profiler that shows us what websites are built with.

it uncovers more than a thousand technologies in dozens of categories such as programming languages, analytics, marketing tools, payment processors, CRM, CDN ...etc..

it can also find out what CMS a website is using, as well as any framework, ecommerce platform, JavaScript libraries and many more.

# Site report for <https://www.ssn.edu.in>

► 🔍 Look up another site?

Share: [📧](#) [✕](#) [f](#) [in](#) [y](#)

## Background

Site title	Just a moment...	Date first seen	August 2020
Site rank	321315	Primary language	English
Description	Not Present		

## Network

Site	<a href="https://www.ssn.edu.in">https://www.ssn.edu.in</a>	Domain	<a href="https://www.ssn.edu.in">ssn.edu.in</a>
Netblock Owner	Cloudflare, Inc.	Nameserver	pdns.ssn.edu.in
Hosting company	Cloudflare	Domain registrar	registry.in

Ref Link: <https://sitereport.netcraft.com/?url=https://www.ssn.edu.in>

The screenshot shows the homepage of ssn.edu.in. The header includes navigation links for 'Lateral Entry Admissions 2024', 'M.E/M.Tech Admissions 2024', and 'Scholarship'. The main banner features the ssn logo, the text 'SHAPING TOMORROWS *Innovators*', and 'M.E / M.TECH ADMISSIONS 2024'. A woman is shown holding a book titled 'COMPUTERS AS COMPONENTS'. A 'NOW OPEN' badge is visible. The Wappalyzer overlay on the right lists the following technologies:

- CMS:** WordPress 5.3.6
- Widgets:** Slider Revolution 6.2.2
- Photo galleries:** Slider Revolution 6.2.2
- Analytics:** Site Kit 1.48.1, PixelYourSite, Google Analytics GA4
- Tag managers:** Google Tag Manager
- Page builder:** wpBakery
- JavaScript libraries:** LazySizes, jQuery UI 1.11.4, Isotope, cote.js 2.6.12, Select2

## Step ii

❖ Knowing subdomain of a website

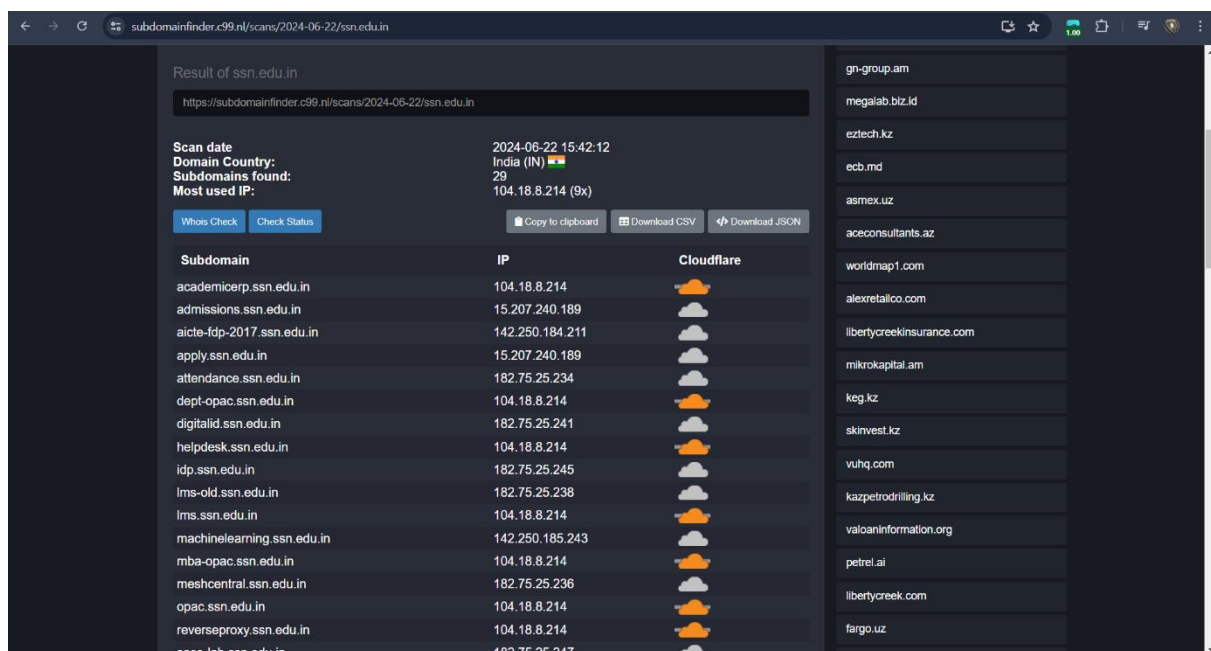
### What is a Subdomain?

A subdomain is a prefix added to a website's domain name to create a separate section of the site. Subdomains are often used to organize and distinguish different types of content or information.

Subdomain increase the scope of an attack

For example, a website owner might use subdomains to separate a blog, online store, or support platform from the rest of the site.

We can locate subdomains using subdomain finder.



From the subdomain finder I was able to list out 21 subdomains but out of which 8 subdomains had no IP and some few subdomains were using webapp filter

## Step iii

### ❖ Find all the URL's on a website

Using link-extractor , this is used to find all the links of a website all in one place

[Tell a Friend](#) [Add to Favorites](#) [Report](#) Share: [g](#) [f](#) [t](#) [p](#) [in](#) [v](#)


**What are Hyperlinks?**  
Hyperlinks, also known as "Links" are used to link pages of the website, documents, etc. together. Links are used to move through the website and/or to other websites, portals, search engines, etc. on the world wide web. They may be image or text based links that point to another location.

**Related Tools:** [JavaScript Extractor](#) | [Email Extractor](#) | [Meta Tags Extractor](#)

**\* Enter URL**   
(e.g. http://www.website.com) [Extract](#)

**Show Links:** ☒ All ☐ Inbound ☐ Outbound ☐ Unbound

**Options:** ☒ Display Categorized List of URLs  
☒ Convert Relative URLs to Absolute URLs  
☒ Show general attributes like: 'title', 'anchor text' or 'alt' tag etc.

 **Can't reach URL: https://www.ssn.edu.in/**

Unfortunately my college website couldn't respond back . it was unable to fetch all the link related to ssn.edu.in is because the home page responds 403 HTTP status code

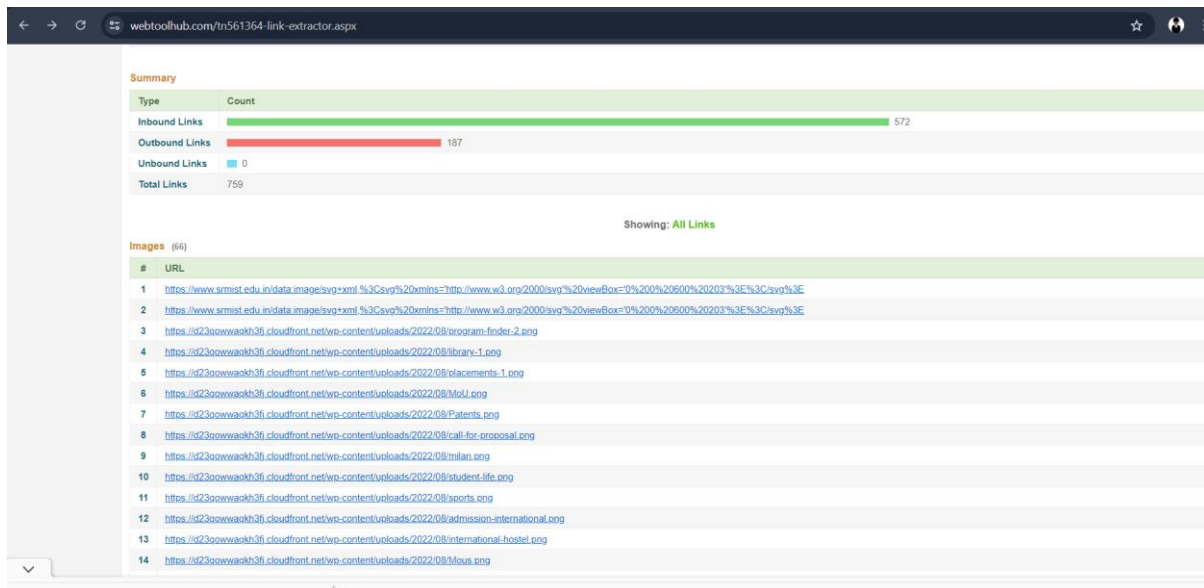
So I switched to another college's website (https://www.srmist.edu.in/)

**Related Tools:** [JavaScript Extractor](#) | [Email Extractor](#) | [Meta Tags Extractor](#)

**\* Enter URL**   
(e.g. http://www.website.com) [Extract](#)

**Show Links:** ☒ All ☐ Inbound ☐ Outbound ☐ Unbound

**Options:** ☒ Display Categorized List of URLs  
☒ Convert Relative URLs to Absolute URLs  
☒ Show general attributes like: 'title', 'anchor text' or 'alt' tag etc.



So as we can see that it has extracted all the link with respect to that main webpage.

## **Step iv**

### ❖ Finding the security headers

When ever we start developing a website we have to take proper security measures with respect to how the authentication is being carried out and how information is being between each sessions, how do we prevent from some small attacks with security headers

### **What are Security headers?**

Security headers are directives used by web applications to configure security defenses in web browsers. Based on these directives, browsers can make it harder to exploit client-side vulnerabilities such as Cross-Site Scripting or Clickjacking.

In general, Headers are the information that is given to a packet . so whenever a packet comes to a website it first analyses the packet then check how the packet is communicating with the website.

So to find if security headers has been implemented or not we can visit [securityheaders.com](https://securityheaders.com)

The screenshot shows a web browser window with the URL `securityheaders.com/?q=https%3A%2F%2Fwww.ssn.edu.in%2F&followRedirects=on`. The page displays a "Security Report Summary" for the site `https://www.ssn.edu.in/`. The report includes the IP address `2606:4700::6812:8d6` and the report time `30 Jun 2024 17:33:03 UTC`. Under the "Headers" section, six missing headers are listed with red "X" icons: `Strict-Transport-Security`, `Content-Security-Policy`, `X-Frame-Options`, `X-Content-Type-Options`, `Referrer-Policy`, and `Permissions-Policy`. An "Advanced" section states, "Ouch, you should work on your security posture immediately," with a "Start Now" button. Below the summary is a "Missing Headers" table with descriptions for each missing header, and a "Raw Headers" section at the bottom.

Header	Description
<code>Strict-Transport-Security</code>	<code>HTTP Strict Transport Security</code> is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value " <code>Strict-Transport-Security: max-age=31536000; includeSubDomains</code> ".
<code>Content-Security-Policy</code>	<code>Content Security Policy</code> is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
<code>X-Frame-Options</code>	<code>X-Frame-Options</code> tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value " <code>X-Frame-Options: SAMEORIGIN</code> ".
<code>X-Content-Type-Options</code>	<code>X-Content-Type-Options</code> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content type. The only valid value for this header is " <code>X-Content-Type-Options: nosniff</code> ".
<code>Referrer-Policy</code>	<code>Referrer Policy</code> is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
<code>Permissions-Policy</code>	<code>Permissions Policy</code> is a new header that allows a site to control which features and APIs can be used in the browser.

so from the analysis we can see that (<https://www.ssn.edu.in/>) has the following 6 headers missing

most developers miss out on this feature , until and unless an application security team tells them to add security header, it is always best nd effective to add security headers while implementing the code .

Strict transport security :- HTTP Strict Transport Security (HSTS) is a simple and widely supported standard to protect visitors by ensuring that their browsers always connect to a website over HTTPS.

Content-Security-Policy :-Content-Security-Policy is the name of a HTTP response header that modern browsers use to enhance the security of the document (or web page). The Content-Security-Policy header allows you to restrict which resources (such as JavaScript, CSS, Images, etc.) can be loaded, and the URLs that they can be loaded from.

X-Frame-options:- The X-Frame-Options header can be used to control whether a page can be placed in an IFRAME. Because the Frame-sniffing technique relies on being able to place the victim site in an IFRAME, a web application can protect itself by sending an appropriate X-Frame-Options header.



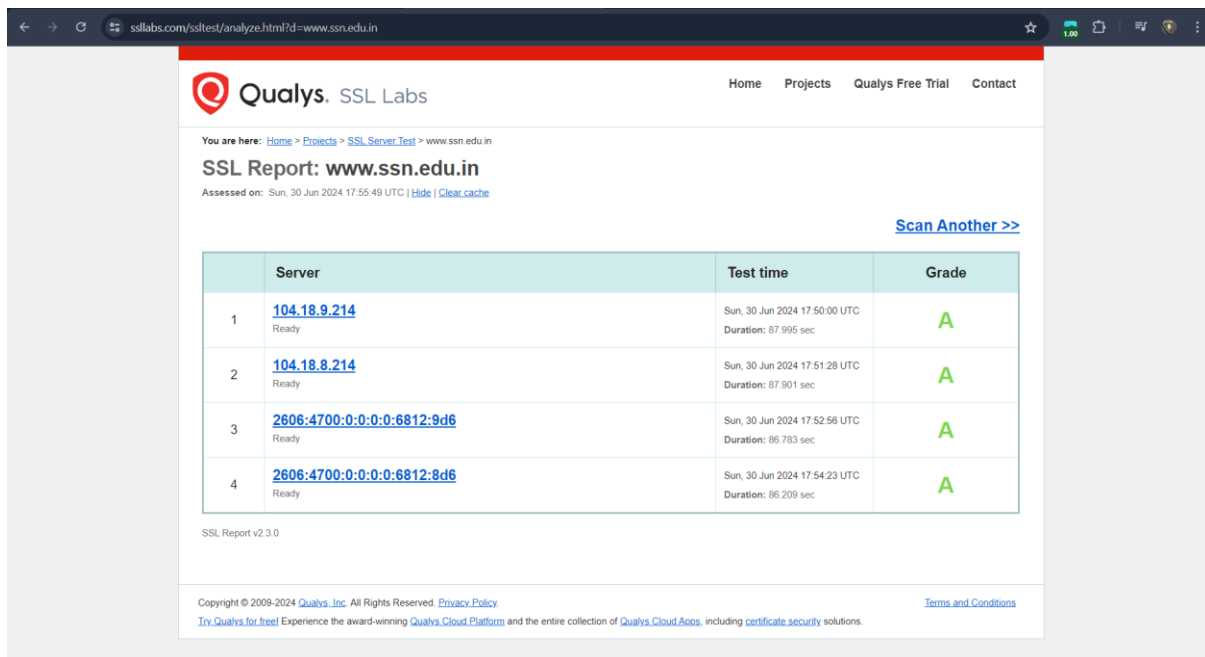
## Step v

### ❖ SSL / TLS test

For the HTTPS protocol to operate securely(S) , the functionality is give by Transport Layer Security (TLS) and Secure Socket Layer(SSL). This encrypts the communication

In modern day current scenario we use TLS version1.2 &1.3

To check the SSL we can visit SSLlabs.com from a popular vendor called Qualys.



	Server	Test time	Grade
1	<a href="#">104.18.9.214</a> Ready	Sun, 30 Jun 2024 17:50:00 UTC Duration: 87.995 sec	A
2	<a href="#">104.18.8.214</a> Ready	Sun, 30 Jun 2024 17:51:28 UTC Duration: 87.901 sec	A
3	<a href="#">2606:4700:0:0:0:0:6812:9d6</a> Ready	Sun, 30 Jun 2024 17:52:56 UTC Duration: 86.783 sec	A
4	<a href="#">2606:4700:0:0:0:0:6812:8d6</a> Ready	Sun, 30 Jun 2024 17:54:23 UTC Duration: 86.209 sec	A

SSL Report v2.3.0

Copyright © 2009-2024 [Qualys, Inc.](#) All Rights Reserved. [Privacy Policy](#) [Terms and Conditions](#)  
[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.

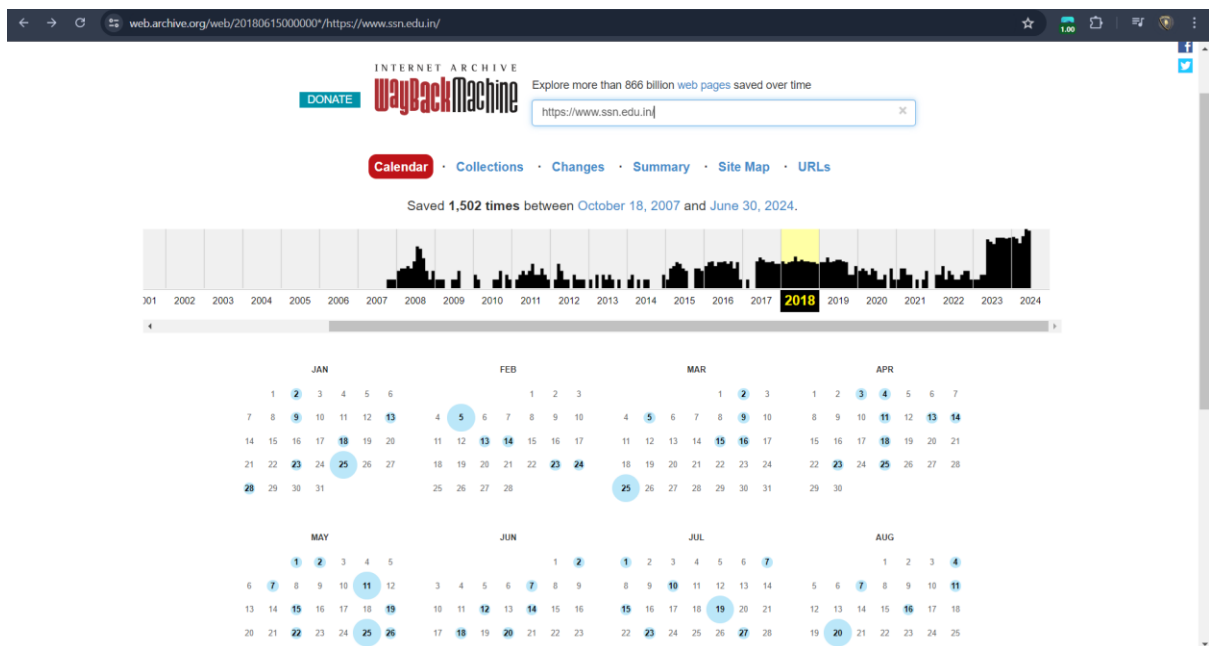
## Step vi

### ❖ Time travel across a website

As we view the website that is updated with 2024 but what if we wanted to take a look at the same website and see what it was like few years ago.

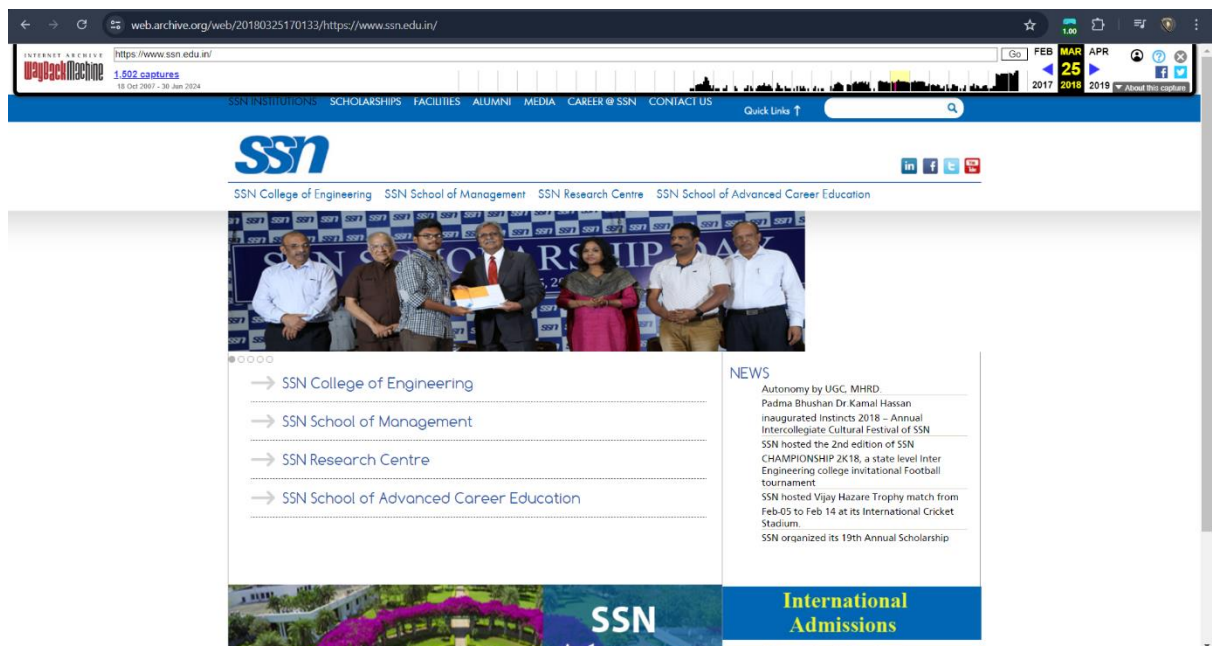
In our older website there is a slight chance that the company/institute may have given out some vulnerable data like employees email or some other personal data that could potentially be vulnerable . so this Time travel is accomplished by ‘wayback machine’(archive.org)

Ref: ([https://web.archive.org/web/20240000000000\\*/https://www.ssn.edu.in/](https://web.archive.org/web/20240000000000*/https://www.ssn.edu.in/))



The snapshots of the each date , year and month is highlighted within the time frame and anyone can look upon that data .

This is the same website [ssn.edu.in](https://www.ssn.edu.in/) that this is how it looked during March-25-2018



## Step vii

### ❖ Finding the buffer size of a website

In general 'Buffer size' refers to the Maximum size that a packet can take to a website.

The entire packets are usually fragmented and sent to the destination

```
C:\Users\ryoge>ping www.ssn.edu.in -4

Pinging www.ssn.edu.in.cdn.cloudflare.net [104.18.8.214] with 32 bytes of data:
Reply from 104.18.8.214: bytes=32 time=8ms TTL=52
Reply from 104.18.8.214: bytes=32 time=9ms TTL=52
Reply from 104.18.8.214: bytes=32 time=12ms TTL=52
Reply from 104.18.8.214: bytes=32 time=8ms TTL=52

Ping statistics for 104.18.8.214:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 12ms, Average = 9ms
```

As we can see that the packets got fragmented into 32 bytes each

So let's say I don't want to fragment my packets so in the command prompt I can set the buffer size by using (-l size) and to send the packet as a whole use (-f) so that it does not fragment the packet

```
C:\Users\ryoge>ping -l 1470 -f 104.18.8.214

Pinging 104.18.8.214 with 1470 bytes of data:
Reply from 104.18.8.214: bytes=1470 time=5ms TTL=52
Reply from 104.18.8.214: bytes=1470 time=7ms TTL=52
Reply from 104.18.8.214: bytes=1470 time=6ms TTL=52
Reply from 104.18.8.214: bytes=1470 time=6ms TTL=52

Ping statistics for 104.18.8.214:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 7ms, Average = 6ms

C:\Users\ryoge>ping -l 1475 -f 104.18.8.214

Pinging 104.18.8.214 with 1475 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 104.18.8.214:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

As we can see that it supported until 1470 bytes and was able to communicate without fragmenting but as soon as I increased the buffer size to 1475 it declined to communicate and prompts us to fragment the packet.

So why does this buffer size matter ?

While DOS attack – Hackers send artificial traffic to disrupt the services and communication of that website

Buffer size affects speed and wear more in some apps than others, but any time the buffer is exceeded, you lose both performance and durability

# **SUMMARY**

## **Project Overview:**

The footprinting project was conducted as part of a mini project in Cyber Security under the ACMEGRADE internship(April 2024 batch) Date: 30-06-2024. The aim was to gather intelligence on the SSN College of Engineering website (ssn.edu.in) to identify potential vulnerabilities, using ethical and educational methodologies.

## **Objectives:**

- To understand the structure and technologies used by the target website.
- To identify potential security gaps and suggest improvements.
- To gain practical experience with various footprinting tools and techniques.

## **Methodologies and Tools:**

### **1. Social Media Reconnaissance:**

Utilized platforms such as Facebook, Instagram, and Twitter to gather basic information about the college, courses offered, and upcoming events.

### **2. Ping and Traceroute Commands:**

Performed basic network tests to check the responsiveness and latency of the website.

### **3. Hacking Search Engines:**

Shodan-Identified web technologies, open ports, and other relevant information.

Technologies found included LinkedIn Ads, Adobe Experience Manager, OneTrust, jQuery, and Java.

Open ports: 80, 443, 2082, 2083, 2086, 2087, 2096, 8080, 8443, 8888.

Censys- Provided detailed descriptions of each open port, including status, body hash, HTML title, and response body.

#### 4. Google Dorking:

Used advanced Google search queries to find specific file types and sensitive information that could be unintentionally exposed on the website.

#### 5. Website Technologies Identification:

Netcraft- Analyzed site information and cybercrime protection measures.

Wappalyzer- Profiled website technologies including CMS, JavaScript libraries, and programming languages.

#### 6. Subdomain Enumeration:

Identified 21 subdomains, though some lacked IP addresses or were filtered by web applications.

#### 7. Link Extraction:

Attempted to extract all URLs on the website using link-extractor tools but faced restrictions due to a 403 HTTP status code.

#### 8. Security Headers Analysis:

Used securityheaders.com to check for missing security headers. Found that the site lacked important headers such as Strict Transport Security, Content-Security-Policy, and X-Frame-Options.

#### 9. SSL/TLS Testing:

Conducted SSL tests using Qualys SSL Labs to ensure secure HTTPS communication.

#### 10. Wayback Machine Analysis:

- Used archive.org to view historical snapshots of the website, identifying potential past vulnerabilities.

#### 11. Buffer Size Testing:

- Tested the maximum buffer size the website could handle without fragmenting packets, which is crucial for defending against Denial of Service (DoS) attacks.

### **Findings and Recommendations:**

- Open Ports: Several open ports were identified, which could be potential entry points for attacks. It's recommended to review and close unnecessary ports.
- Security Headers: The absence of key security headers could leave the site vulnerable to attacks like Cross-Site Scripting (XSS) and Clickjacking. Implementing these headers is critical.
- SSL/TLS Configuration: Ensuring the latest SSL/TLS protocols are in use to maintain secure communications.
- Historical Data: Reviewing and securing old versions of the site to prevent exposure of outdated and potentially vulnerable information.

### **Conclusion:**

The footprinting exercise on the SSN College of Engineering website provided valuable insights into its security posture. By identifying open ports, missing security headers, and analyzing historical data, recommendations were made to enhance the website's security. This project underscored the importance of continuous monitoring and updating of security measures to protect against evolving cyber threats.

This report of mine(R.Yogeshram) reflects the comprehensive approach taken to assess and improve the security of the SSN College of Engineering website.