

So, basically Reconnaissance or foot printing are of two types in which Hackers gather information. They are :

► **BASIC RECONNAISSANCE**: This are very basic things which a hacker usually does for gathering information. They are by:

1. **Social Networking Sites**: Through social networking sites one can gather a bunch of information required of a company for hacking into it.

2. **Hacking Search Engines**: It helps to get much deeper information about a particular company that a normal search engines can't fetch just by coping the companies IP address and pasting in the hacking search engines. Some of it are Shodan, Censys, Notevil, Duckduckgo.

3. **Google Dorks**: It helps to search for a precise or a specific information that you are looking for.

► **ADVANCE RECONNAISSANCE** : This are some advance techniques which a hacker usually use for gathering information. They are by:

1. **Website Technology Extension** : This helps to find loop holes while developing websites. Some of it are “netcraft” and “wapplyzer”.

2. **Subdomains Of Websites** : This helps to find subdomains of all the main domains. Thus making easy for Hacker to find loop holes and get into the environment. “subdomain finder” finds the subdomains of all the domains.

3. **Hidden Links Of Website** : This helps to get all additional links that a particular website bears which are hidden from public. “link extractor” helps in doing so.

4. **Check Security Headers Of a Website** : This checks the packet information by “securityheaders.com”.

5. **SSL Test** : One can test their secure socket layers through “ssllabs.com” or “sslltest.com”.

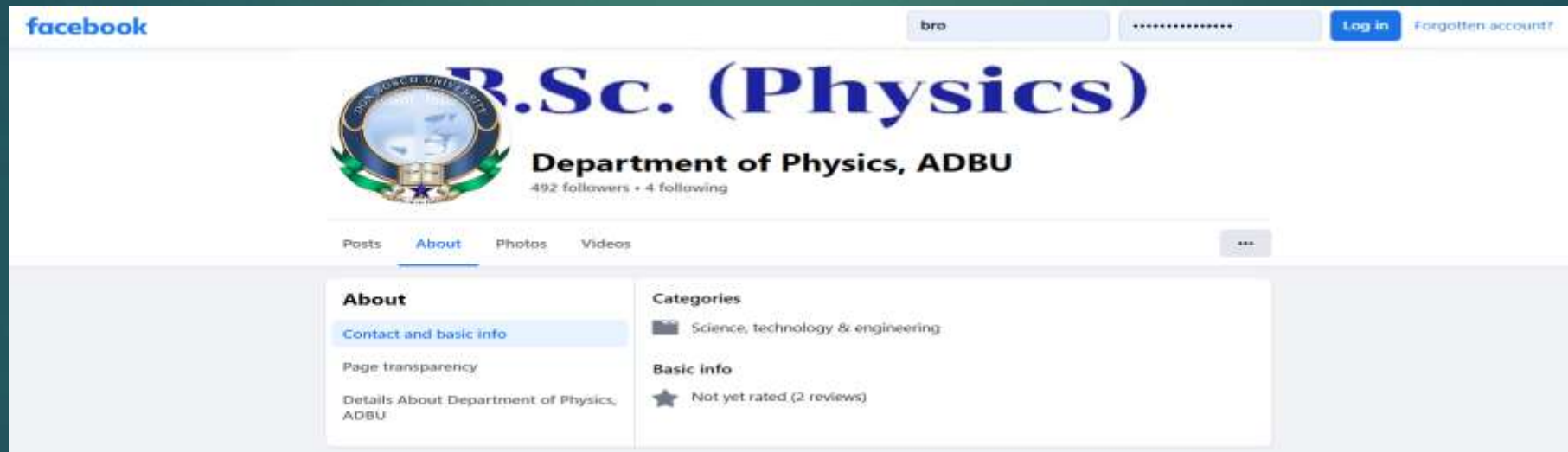
6. **IP Of a Website and Buffer Size** : One can search for IP address of a website through command prompt and the buffer size which is the maximum size of the packets.

7. **Time Travel Over a Website** : It is also called as time way back machine. It helps to gather some of the personal information about a particular website through travelling back in time when the particular website was developed.

“archive.org” helps in doing so.

So lets perform some Basic Reconnaissance in my university website.

- **Social Networking Sites** : Some information gathered through social networking sites of my university are as follows –





assamdonboscouniversity

Follow

95 posts

575 followers

0 following

ADBU MEDIA

Department of Mass Communication, Assam Don Bosco University
www.dbuniversity.ac.in



Special Lectur...



Special Days



Studio

Assam Don Bosco University, Guwahati, Assam

Carpe Diem! Life in its fullness!

Education Administration Programs · Guwahati, Assam · 911 followers



1 person from your school works here · 64 employees

✓ Following

Visit website

More

Home

About

Posts

Jobs

Alumni

Overview

Assam Don Bosco University

Assam Don Bosco University (ADBU) is established as the first State University of Assam in the private sector on 29 March 2008, and set up by Don Bosco Society in response to the felt educational needs of the people of North-East India. In a little over 10 years, Assam Don Bosco University has become one of the best Universities in the Northeast and has the distinction of the only private University in Assam with an 'A' Grade from National Assessment and Accreditation Council (NAAC). The University has also been given a 12B status by the University Grants Commission, hence, becoming the first private University to attain this status in North East and the fourth in the country.

Website

<http://www.dbuniversity.ac.in>

- **Hacking Search Engines** : By the IP address of my university I can get much deeper information that normal search engines cant give.

By Using Shodan we can see the ports of my university that are open:

The screenshot displays the Shodan search results for the IP address 172.67.71.238. The interface is dark-themed. At the top, the IP address is prominently displayed in a white box. Below it, there are tabs for 'Regular View', 'Raw Data', and 'History'. A satellite map of San Francisco is visible in the background. The main content is divided into two columns. The left column, titled 'General Information', lists various details about the IP: Hostnames (escapehunt.com, snl.cloudflaressl.com), Domains (ESCAPEHUNT.COM, CLOUDFLARESSL.COM), Country (United States), City (San Francisco), Organization (Cloudflare, Inc.), ISP (Cloudflare, Inc.), and ASN (AS13335). The right column, titled 'Open Ports', shows a list of open ports: 80, 443, 2052, 2053, 2082, 2086, 2087, 8080, 8443, and 8880. Below the ports, there is a section for the selected port 80 / TCP, showing the raw data of the connection, including headers like Date, Content-Type, Content-Length, Connection, X-Frame-Options, Referrer-Policy, Cache-Control, Expires, Vary, Server, and CF-RAY.

172.67.71.238

Regular View Raw Data History

// TAGS: cch // LAST SEEN: 2023-03-20

General Information

Hostnames: escapehunt.com, snl.cloudflaressl.com

Domains: [ESCAPEHUNT.COM](#) [CLOUDFLARESSL.COM](#)

Country: United States

City: San Francisco

Organization: Cloudflare, Inc.

ISP: Cloudflare, Inc.

ASN: AS13335

Open Ports

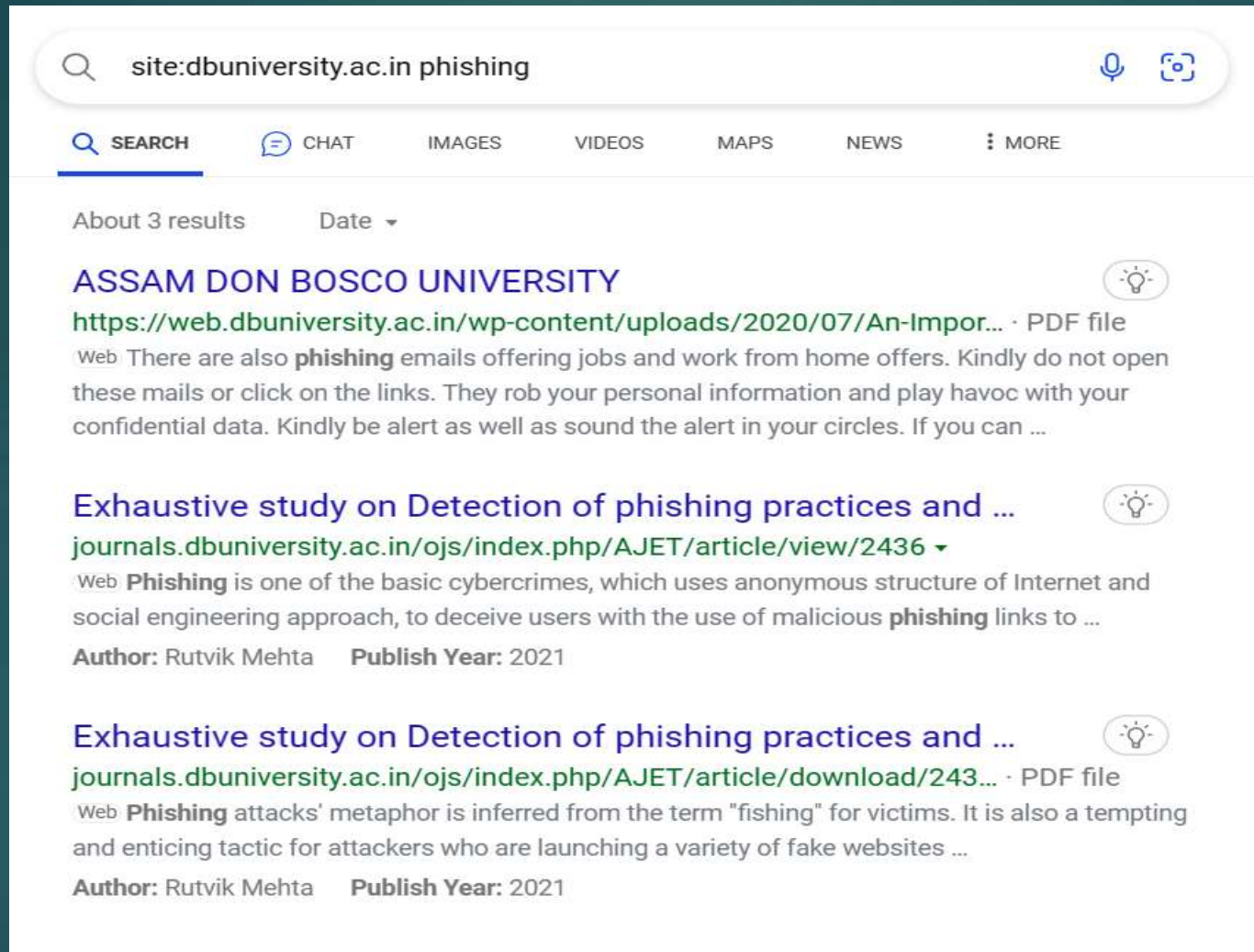
80 443 2052 2053 2082 2086 2087 8080 8443 8880

// 80 / TCP

CloudFlare

HTTP/1.1 403 Forbidden
Date: Sat, 18 Mar 2023 16:54:52 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5854
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 7a9effffc55c26e-VIE

► **Google Dorks** : About a particular information related to my website :



The screenshot shows a Google search interface with the query "site:dbuniversity.ac.in phishing" entered in the search bar. Below the search bar, there are navigation links for SEARCH, CHAT, IMAGES, VIDEOS, MAPS, NEWS, and MORE. The search results are displayed below, showing "About 3 results" and a "Date" filter. The first result is titled "ASSAM DON BOSCO UNIVERSITY" and includes a link to a PDF file: "https://web.dbuniversity.ac.in/wp-content/uploads/2020/07/An-Impor...". The snippet mentions phishing emails offering jobs and work from home offers. The second result is titled "Exhaustive study on Detection of phishing practices and ..." and includes a link to a PDF file: "journals.dbuniversity.ac.in/ojs/index.php/AJET/article/view/2436". The snippet discusses phishing as a basic cybercrime. The third result is also titled "Exhaustive study on Detection of phishing practices and ..." and includes a link to a PDF file: "journals.dbuniversity.ac.in/ojs/index.php/AJET/article/download/243...". The snippet discusses phishing attacks and their metaphor. Both the second and third results list the author as "Rutvik Mehta" and the publish year as "2021".

site:dbuniversity.ac.in phishing

SEARCH CHAT IMAGES VIDEOS MAPS NEWS MORE

About 3 results Date ▾

ASSAM DON BOSCO UNIVERSITY

<https://web.dbuniversity.ac.in/wp-content/uploads/2020/07/An-Impor...> · PDF file

Web There are also **phishing** emails offering jobs and work from home offers. Kindly do not open these mails or click on the links. They rob your personal information and play havoc with your confidential data. Kindly be alert as well as sound the alert in your circles. If you can ...

Exhaustive study on Detection of phishing practices and ...

<journals.dbuniversity.ac.in/ojs/index.php/AJET/article/view/2436> ▾

Web **Phishing** is one of the basic cybercrimes, which uses anonymous structure of Internet and social engineering approach, to deceive users with the use of malicious **phishing** links to ...

Author: Rutvik Mehta **Publish Year:** 2021

Exhaustive study on Detection of phishing practices and ...

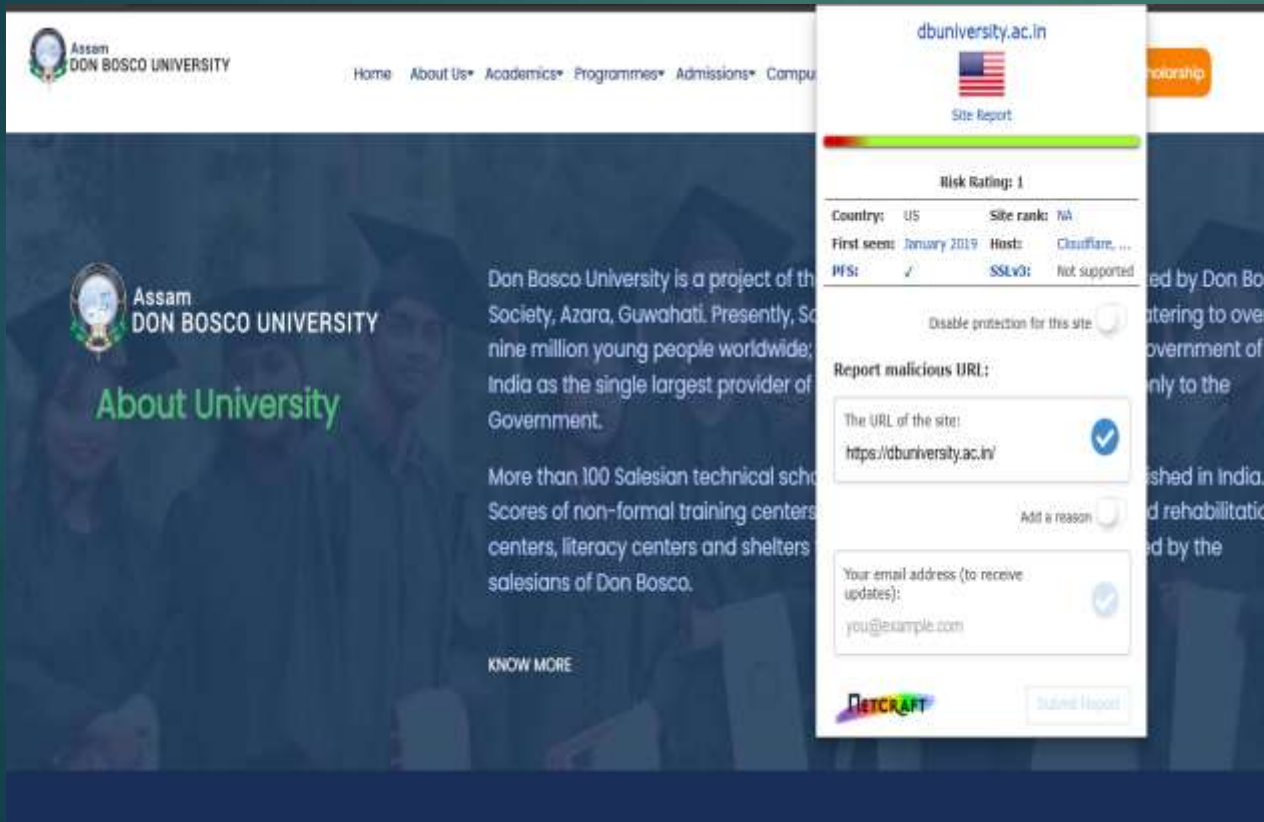
<journals.dbuniversity.ac.in/ojs/index.php/AJET/article/download/243...> · PDF file

Web **Phishing** attacks' metaphor is inferred from the term "fishing" for victims. It is also a tempting and enticing tactic for attackers who are launching a variety of fake websites ...

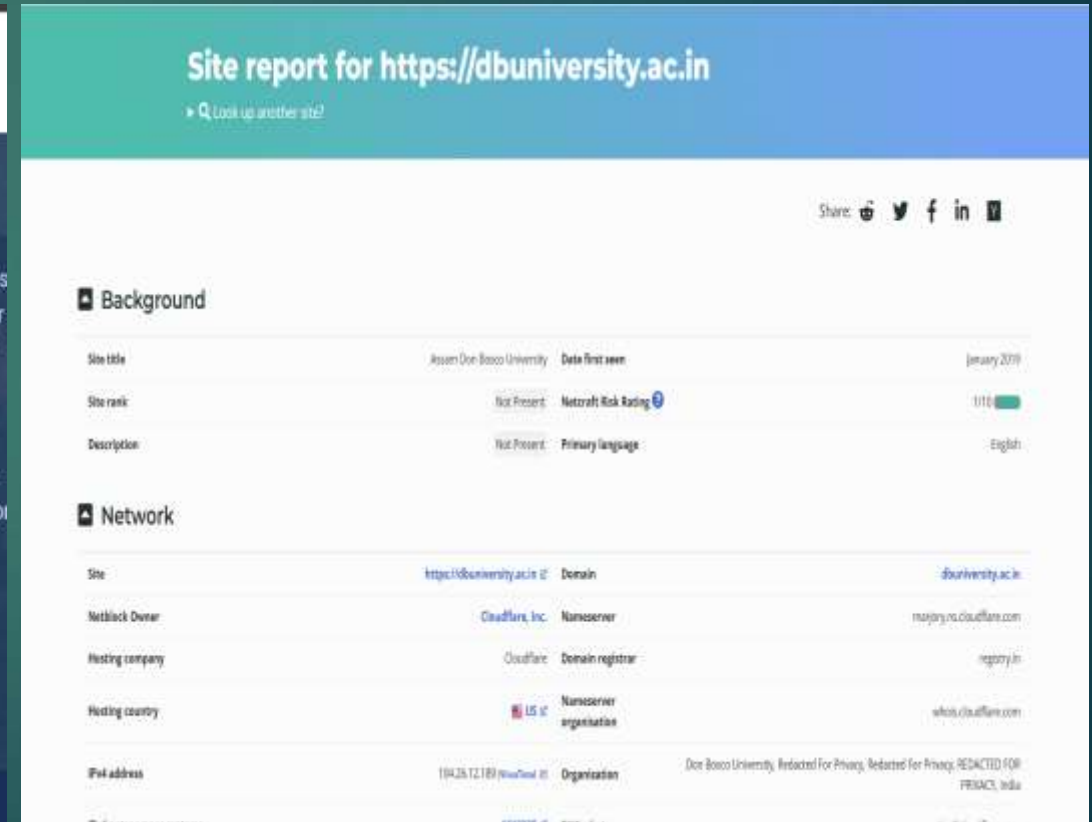
Author: Rutvik Mehta **Publish Year:** 2021

So now lets see some Advance Reconnaissance in my university website.

- **Website Technology** : As by using Netcraft Extension I can find many information related to my university website.



The screenshot shows the homepage of Assam Don Bosco University. A Netcraft site report for dbuniversity.ac.in is overlaid on the page. The report indicates a risk rating of 1, with the site located in the US, first seen in January 2019, and hosted on Cloudflare. The report also shows that SSLv3 is not supported and that the site is not protected for this site. The background of the website features a large image of students and the text "About University".



The screenshot displays a detailed Netcraft site report for <https://dbuniversity.ac.in>. The report includes a "Background" section with site title, rank, and description, and a "Network" section with site, Netcraft owner, hosting company, and IP address. The report also includes a "Share" section with social media links.

Background	
Site title	Assam Don Bosco University
Site rank	Not Present
Description	Not Present

Network	
Site	https://dbuniversity.ac.in
Netcraft owner	Cloudflare, Inc.
Hosting company	Cloudflare
Hosting country	US
IP address	194.25.12.181

IPv4 autonomous systems	AS13335 i2	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:20:0:0:0:681a:cbd	Top Level Domain	India (.ac.in)
IPv6 autonomous systems	AS13335 i2	DNS Security Extensions	unknown
Reverse DNS	unknown		

IP delegation

IPv4 address (104.26.12.189)

IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
1 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
1 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
1 104.26.12.189	United States	CLOUDFLARENET	Cloudflare, Inc.

IPv6 address (2606:4700:20:0:0:0:681a:cbd)

IP range	Country	Name	Description
2606:4700:20:0:0:0:681a:cbd	United States	CLOUDFLARENET	Cloudflare, Inc.

IP delegation			
IPv4 address (104.26.12.189)			
IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
1 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
1 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
1 104.26.12.189	United States	CLOUDFLARENET	Cloudflare, Inc.
IPv6 address (2606:4700:20:0:0:0:681a:cbd)			
IP range	Country	Name	Description
::/96	N/A	ROOT	Root inetBurm object
1 2600::/12	United States	NET5-2600	American Registry for Internet Numbers
1 2606:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
1 2606:4700:20:0:0:0:681a:cbd	United States	CLOUDFLARENET	Cloudflare, Inc.
SSL/TLS			
Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	net.brahmaputra.dbuiversity.ac.in	Supported TLS Extensions	RFC8446 i2 key share, RFC8446 i2 supported versions, RFC4366 i2 server name, RFC7301 i2 application-layer protocol negotiation, RFC6962 i2 signed certificate timestamp, RFC4366 i2 status request

SSL/TLS



Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	net.brahmaputra.dbuniversity.ac.in	Supported TLS Extensions	RFC8446 of key share, RFC8448 of supported versions, RFC4366 of server name, RFC7301 of application-layer protocol negotiation, RFC6962 of signed certificate timestamp, RFC4366 of status request
Organisation	Not Present	Application-Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	Let's Encrypt
Organisational unit	Not Present	Issuer common name	E1
Subject Alternative Name	dbuniversity.ac.in, net.brahmaputra.dbuniversity.ac.in	Issuer unit	Not Present
Validity period	From Feb 1 2023 to May 2 2023 (3 months)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	cloudflare	Issuer state	Not Present
Public key algorithm	id-ecPublicKey	Certificate Revocation Lists	Not Present
Protocol version	TLSv1.3	Certificate Hash	VeE1j4ertj6g5Rt6Br8VmbpH5avw
Public key length	256		

Certificate check

OK

OCSP servers <http://e1o.letsencrypt.org> - 100% uptime in the past 24 hours [View Performance Graph](#)

Signature algorithm

ecdsa-with-SHA384

OCSP stapling response Certificate valid

Serial number

0x0478b3896e7ae83b5aebea8e7f92c75e0e54

OCSP data generated Mar 18 22:00:00 2023 GMT

Cipher

TLS_AES_256_GCM_SHA384

OCSP data expires Mar 25 21:59:58 2023 GMT

Version number

0x02

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Let's Encrypt Oak 2023 tZ773H+Tlp18JnFuLj06P38Qs9NczAE=H8Tg5KtCJk=	2023-02-01 04:26:38	Success
Certificate	Cloudflare Nimbus 2023 eJ0PMN13Lvg6JJgtR17p8RZuH0FTTy5K2E6VW56J1=	2023-02-01 04:26:38	Success

SSLv3/POODLE


This site does not support the SSL version 3 protocol.

[More information about SSL version 3 and the POODLE vulnerability.](#)

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

- **Subdomains of Website** : As I can find many subdomains that my university domain bears through sub domain finder .



Subdomain Finder

Consider helping the project, check out our [Hall of Fame](#)

Start Scan

☒ Private 500k (This makes sure your scan will not be logged, published or indexed. Everything stays private.)

Result of dbuniversity.ac.in

Scan date

Domain Country:

Subdomains found:

Most used IP:

2023-03-20 13:53:58

India (IN) 🇮🇳

182

104.26.13.189 (6x)






























What's Check

Check Status

Copy to clipboard

Download CSV

Download JSON

Subdomain	IP	Cloudflare
alumni.dbuniversity.ac.in	104.26.13.189	
apply.dbuniversity.ac.in	34.220.253.11	
blogs.brahmaputra.dbuniversity.ac.in	167.71.232.59	
brahmaputra.dbuniversity.ac.in	3.111.145.201	
cdn.dbuniversity.ac.in	104.26.12.189	
cisp.dbuniversity.ac.in	104.26.12.189	
conferences.dbuniversity.ac.in	104.26.12.189	
courses.brahmaputra.dbuniversity.ac.in	34.145.189.148	
brahmaputra.dbuniversity.ac.in	3.111.145.201	
cdn.dbuniversity.ac.in	104.26.12.189	
cisp.dbuniversity.ac.in	104.26.12.189	
conferences.dbuniversity.ac.in	104.26.12.189	
courses.brahmaputra.dbuniversity.ac.in	34.145.189.148	
dl.dbuniversity.ac.in	172.67.71.238	
documents.dbuniversity.ac.in	172.67.71.238	
ecampus.brahmaputra.dbuniversity.ac.in	104.26.13.189	
erp.dbuniversity.ac.in	43.242.214.84	
evaluation.brahmaputra.dbuniversity.ac.in	13.233.155.192	
events.dbuniversity.ac.in	104.26.12.189	
exams.brahmaputra.dbuniversity.ac.in	3.108.221.198	
examsadmin.brahmaputra.dbuniversity.ac.in	65.2.33.2	
journals.dbuniversity.ac.in	172.67.71.238	
login.brahmaputra.dbuniversity.ac.in	64.227.138.216	
lult.brahmaputra.dbuniversity.ac.in	162.159.128.53	
meet.dbuniversity.ac.in	14.139.209.86	
moodle.dbuniversity.ac.in	14.139.209.84	
naac.dbuniversity.ac.in	172.67.71.238	
net.brahmaputra.dbuniversity.ac.in	192.0.78.201	
nisp.dbuniversity.ac.in	104.26.13.189	
online.dbuniversity.ac.in	54.212.8.30	
onlineprograms.dbuniversity.ac.in	3.126.202.50	
opac.dbuniversity.ac.in	104.26.13.189	
prajyuktam.dbuniversity.ac.in	104.26.13.189	

Recent scans:

dbuniversity.ac.in

thangkhuymathanoi.vn

chnosatko.vn

smaligroupstours.vn

xuatnhapcanh.com.vn

flatout.com.br

topcity.vn

dyn.vn

vattieuaydung.org.vn

thaibinhvn.vn

dekiru.vn

qgtechno.com.vn

ducanhplastic.com.vn

dekiru.vn

qgtechno.com.vn

ducanhplastic.com.vn

timhieuphapluat.vn

namanhlaptop.vn

congngheleminh.vn

atpshop.vn

minhtran.vn

loa.com.vn

tourism.vn

loakeo.vn

alsoft.vn

hoangphat360.vn

baa.org.vn

cyberweb.vn

cartabergvietnam.vn

reviewbatdongsan.vn

- **Finding hidden links of website** : I can find many hidden links of my university website through “linkextractor” .

URLs				
Plain URLs Internal Links Only External Links Only				
Sr#	URL	Anchor	Follow Status	Type
1	http://dbuniversity.ac.in/	A-	dofollow	Internal Link
2	http://dbuniversity.ac.in/index.php	Image	dofollow	Internal Link
3	http://dbuniversity.ac.in//cdn-cgi/l/email-protection	[email protect ed]	dofollow	Internal Link
4	https://www.youtube.com/user/ADBUGuwahati	Youtub e	dofollow	External Link
5	https://twitter.com/DonBoscoUniv	Twitter	dofollow	External Link
6	https://www.facebook.com/AssamDonBoscoUniversity/	Faceb ook	dofollow	External Link
7	http://dbuniversity.ac.in//dbuglobal	Dista nce Educat ion	dofollow	Internal Link
8	http://dbuniversity.ac.in/javascript:void(0)	about us	dofollow	Internal Link


- ▶ **Checking Security Headers of Website :** As you can see I can find many security Headers missing for my university website as I checked through “securityheaders.com”.

Scan your site now

Scan

☐ Hide results ☒ Follow redirects

Security Report Summary



Site: <http://104.26.12.189/> - (Scan again over https)

IP Address: 104.26.12.189

Report Time: 20 Mar 2023 12:58:37 UTC

Headers: ✓ X-Frame-Options ✓ Referrer-Policy ✗ Content-Security-Policy ✗ X-Content-Type-Options
✗ Permissions-Policy

Warning: Grade capped at A, please see warnings below.

- **SSL Test :** As the certificates in each of the server of my university is fine and can be checked through “sslltest.com”.

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > dbuniversity.ac.in

SSL Report: dbuniversity.ac.in

Assessed on: Mon, 20 Mar 2023 13:18:30 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	104.26.13.189 Ready	Mon, 20 Mar 2023 13:03:12 UTC Duration: 147.477 sec	A
2	104.26.12.189 Ready	Mon, 20 Mar 2023 13:05:39 UTC Duration: 146.809 sec	A
3	2606:4700:20:0:0:0:ac43:47ee Ready	Mon, 20 Mar 2023 13:08:06 UTC Duration: 147.16 sec	A
4	172.67.71.238 Ready	Mon, 20 Mar 2023 13:10:33 UTC Duration: 172.679 sec	A
5	2606:4700:20:0:0:0:681a:dbd Ready	Mon, 20 Mar 2023 13:13:26 UTC Duration: 157.335 sec	A
6	2606:4700:20:0:0:0:681a:cbd Ready	Mon, 20 Mar 2023 13:16:03 UTC Duration: 146.564 sec	A

- **IP Address and Buffer size** : I can get to know the buffer size through the command prompt.

```
C:\Users\Aman>ping -f -l 1470 104.26.12.189

Pinging 104.26.12.189 with 1470 bytes of data:
Reply from 104.26.12.189: bytes=1470 time=307ms TTL=56
Reply from 104.26.12.189: bytes=1470 time=214ms TTL=56
Reply from 104.26.12.189: bytes=1470 time=215ms TTL=56
Reply from 104.26.12.189: bytes=1470 time=217ms TTL=56

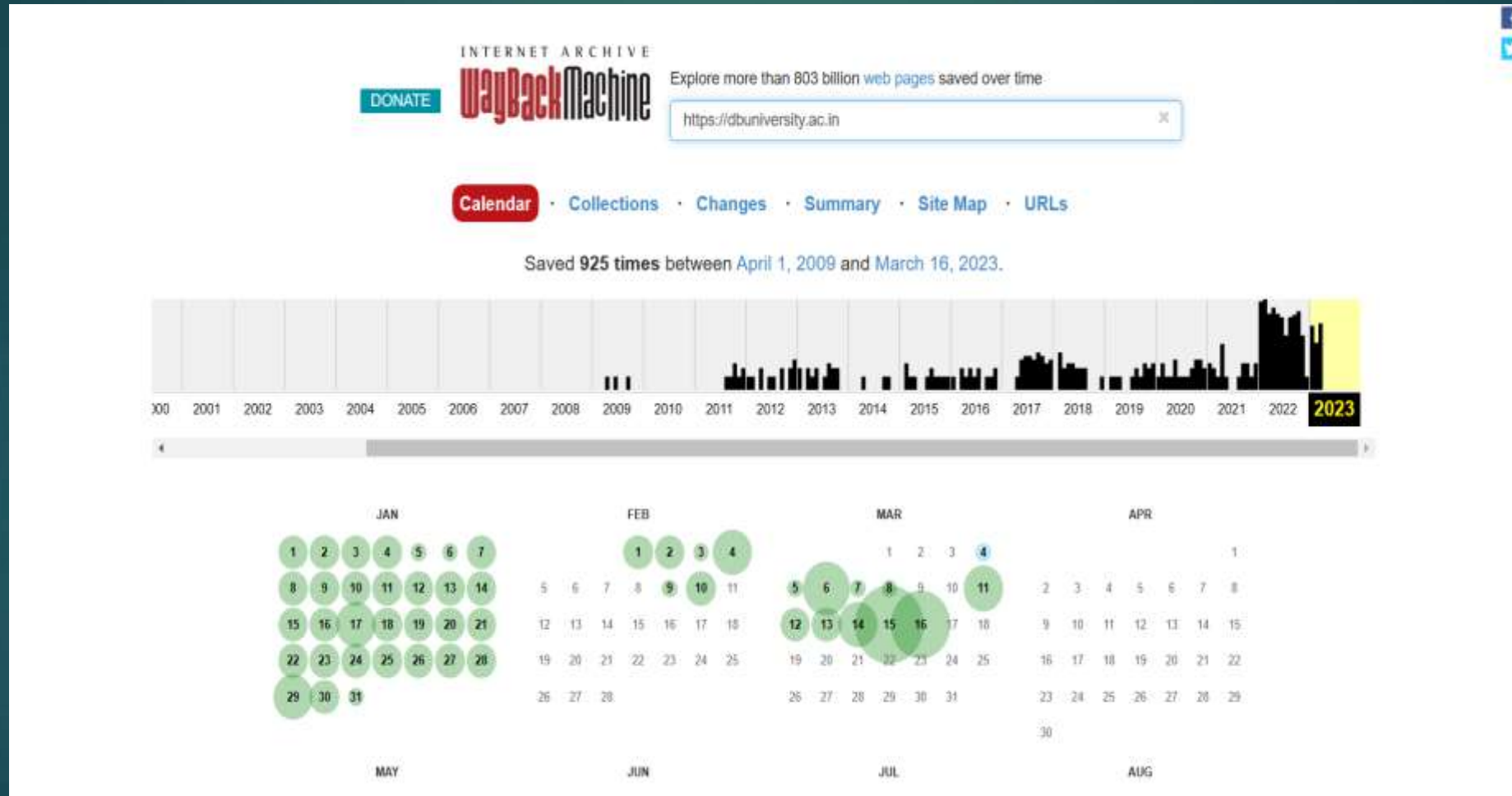
Ping statistics for 104.26.12.189:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 214ms, Maximum = 307ms, Average = 238ms

C:\Users\Aman>ping -f -l 1475 104.26.12.189

Pinging 104.26.12.189 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 104.26.12.189:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- **Time Travelling** : I can also time travel on my university website and find some personal details there.



THANK YOU