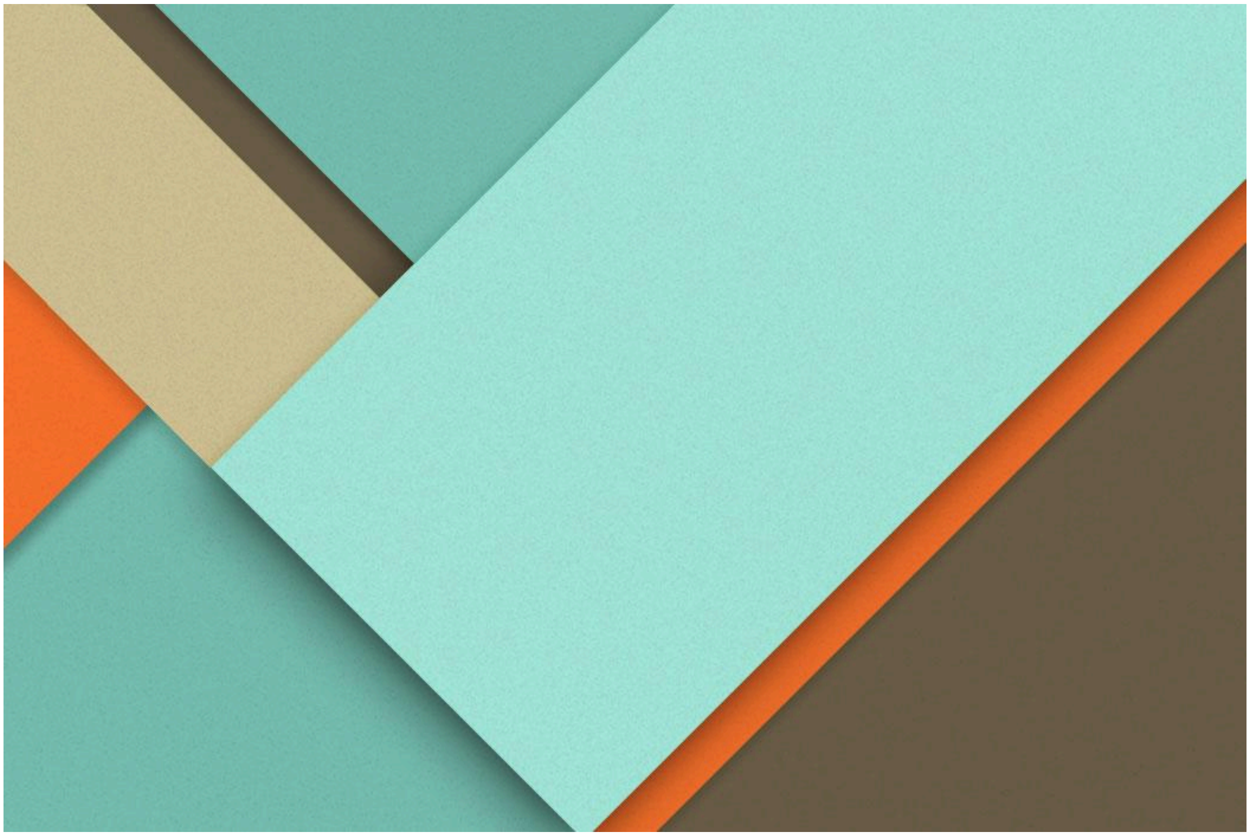

Project– Footprinting And Reconnaissance

01.01.2025

MUHAMMED SAFAYATH T
suhailariyallur1@gmail.com
Kerala
IIT INDORE - INTELLIPAAT
STUDENT

Overview

THIS PROJECT IS A COMPREHENSIVE RECONNAISSANCE ON THE TARGET INTELLIPAAT.COM

Goals

1. Understand RECON in depth
2. Covers Various RECON tools from beginner to intermediate
3. Points our specific vulnerabilities and solutions .

Tasks to be Performed:

1. Internet Presence Analysis: Explore Intellipaat's website, social media pages, and mentions in blogs and news stories to gauge their online presence and reputation. Pay special attention to any negative publicity or customer reviews that could affect the company's image.

2. HTTP Header Inspection: Examine the HTTP headers of Intellipaat’s website. Determine how the information obtained from these headers can be valuable for footprinting and potentially revealing details about the server setup and technology in use.

3. Metadata Analysis: Find a public figure or a popular place and investigate how crucial information about them can be discovered in the metadata of photos uploaded on social media. Share the specific information you retrieve.

4. Domain Information: Obtain details about the Intellipaat domain name, including the registrar, registration date, expiration date, and name servers associated with the domain.

5. Email Address Research: Investigate the support@intellipaat.com email address to discover more about the owner, searching through publicly accessible materials such as web pages, forums, and social media accounts. Share any relevant findings.

6. WHOIS Lookup: Perform a WHOIS lookup to find out who owns intellipaat.com and provide details such as the registrant's name, organization, email address, and phone number.

7. Subdomain Enumeration: List all of Intellipaat's subdomains and explain the methods or tools you used to find them.

Solution:-

1-INTERNET PRESENTS ANALYSIS :-

Intellipaat is well present across the World wild web

Sherlock tool can directly show that .
Sherlock intellipaat.com

SEO performance using PAGESPEED INSIGHT:
Core Web Vitals (CWV) assessment failed:-
https://pagespeed.web.dev/analysis/https-intellipaat-com/7z1c4pakr2?form_factor=mobile
https://pagespeed.web.dev/analysis/https-intellipaat-com/7z1c4pakr2?form_factor=desktop
in Desktop session:-
FACTORS CONTRIBUTING LESS PERFORMANCE FOR THE WEBSITE AS PER PAGESPEED DATA:-
FCP - 2.0s , It have to be less than 1.8s
LCP - 2.6S , It have to be less than 2.5s
SEO - 85 which is okay but will better if improved
in mobile session:-
There are several factors limiting the performance of websites affecting user experience from being best.as it is a low limitation but comparing with other competitors still need improvement . CWV failure seems common in mobile experience , but some competitors have passed in at least desktop experience .

2-HTTP HEADER inspection:-

SCANNED BY SECURITYHEADER.COM , IT SAYS THERE IS A MISSING HEADER NAMED “Permission-Policy”

```
https://securityheaders.com/?q=intellipaat.com&hide=on&followRedirects=on
HTTP/2 200 OK
Date: Wed, 01 Jan 2025 12:26:01 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Pragma: no-cache
Access-Control-Allow-Origin: https://lms.intellipaat.com
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-transform, no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=2592000; includeSubDomains; preload
Cf-Cache-Status: DYNAMIC
Set-Cookie:
___cf_bm=IwU3NWCqlCtQkX7pqybxyGzAiX9v57YUswUUQB2Hhp4-1735734361-1.0.1.
1-kmMYYECsKmXbLX9uODT.yxXaf7GGHUv_7FPE4LcYr_87rTd_QLHt9oK6Lp9dY7r
99uprLYVbag0ozZ1lnoLXTA; path=/; expires=Wed, 01-Jan-25 12:56:01 GMT;
domain=.intellipaat.com; HttpOnly; Secure; SameSite=None
Content-Security-Policy: frame-ancestors 'self' *.intellipaat.com google.com
zopim.com facebook.com doubleclick.net zoho.com tagmanager.google.com
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Server: cloudflare
Cf-Ray: 8fb27ec81a94d5a1-AMS
Alt-Svc: h3=":443"; ma=86400.
```

VALUABLE INFORMATION I GOT :-

Cookies says the website is built with PHP , also Wordpress
This header says server is CDN - cloudflare located routed through Amsterdam data centre.
SameSite=None :-This can allows the cookie to be sent with cross-site requests.SameSite=None is acceptable if cross-site functionality is necessary (e.g., Cloudflare bot protection)..

3-METADATA:-

Technology
Built with -
https://builtwith.com/intellipaat.com
https://builtwith.com/meta/intellipaat.com :- it gives metadata about the website and usage and employees etc..
Wappalizer :-

Wappalizer gives a lot of information about website and it built with
Like data base- Mysql ,and several details

4-DOMAIN INFO:-

Can use tools like:-
Censys.io , shodan.io
Nslookup , whois , viewdrs.info for reverse lookup , centralops.net ,
From whoxy.com :-
Domain: INTELLIPAAT.COM (16 similar domains)
Registrar: GoDaddy.com, LLC (146 million domains)
Query Time: 1 Jan 2025 - 2:50 PM UTC [LIVE WHOIS]
Registered: 4th April 2011 [13 years, 8 months, 28 days back]
Updated: 26th March 2024 [9 months, 6 days back]
Expiry: 4th April 2026 [1 year, 3 months, 2 days left]

5-EMAIL ADDRESS RESEARCH:

support@intellipaat.com email Address is valid , using website:- verifalia.com
DATA BREACHES:-
2 DATA BREASHES FOUND IN WEBSITE haveibeenpwned.com. for the domain support@intellipaat.com
1-IIMJobs: In December 2018
2-Combolists Posted to Telegram

6-WHOIS LOOKUP:

Whois and reverse whois lookup.

7-SUBDOMAIN ENUMERATIONS:-

TOOLS:-
Dnsdumpster.com
Sublist3r -d intellipaat.com
https://crt.sh :- Search for subdomains in public SSL/TLS certificates.
Virustotal.com :- Negative Review in community -
https://www.virustotal.com/gui/domain/intellipaat.com/community
And can see dns records :-
https://www.virustotal.com/gui/domain/intellipaat.com/details
theHarvester -d intellipaat.com -b all -l 100
ffuf -w wordlist.txt -u https://FUZZ.intellipaat.com

Asset finder —subs-only intellipaat.com
Dnsrecon -d intellipaat.com -t brt

Note -

The Recon Scanning results has provided in text file