ASSIGNMENT-1 Report

ON

DNS DUMP STACKER

B.E.(IT) V -Sem

BY

APPALA MEENAKSHI SINDHUJA
(160123737001)

UNDER THE GUIDANCE OF

Mr. U.SAI RAM

Assistant Professor
IT Department, CBIT.

DEPARTMENT OF INFORMATION TECHNOLOGY
CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (A)
(Affiliated to Osmania University; Accredited by NBA and NAAC, ISO 9001:2015
Certified Institution), GANDIPET, HYDERABAD – 500 075
Website: www.cbit.ac.in
2024-25

CERTIFICATE

This is to certify that the project work entitled "**DNS DUMPSTACKER**" submitted to CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY, in partial fulfillment of the requirements for the completion of Assignment-1 in V Sem of B.E. In Information Technology during the Academic Year 2024-25, is a record of original work done by Appala Meenakshi Sindhuja during the period of study in the Department of IT, CBIT, Hyderabad.

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Table 1	Address Records
Table 2	MX records
Table 3	NS REcords

LIST OF ABBREVIATIONS

DNS: Domain Name System

IP:Internet Protocol

ASN:Autonomous System Network

ICANN:Internet Corporation for Assigned Names and Numbers

AS112: Autonomous System 112

CDN: Content Delivery Network:

FTP:File Transfer Protocol

A: Address

MX:Mail Exchange

NS:Name Server

TXT:Text

ABSTRACT

This report details the findings from a DNS analysis of the iana.org domain using the DNSDumpster tool. The objective is to provide a comprehensive overview of the domain's DNS records, including A records, MX records, NS records, and TXT records, to understand its public-facing infrastructure from a reconnaissance perspective.

Tool explored:DNSDUMPSTER

A free online domain research tool that can discover hosts related to a domain. It provides a visual representation of DNS records and network mapping, which is crucial for understanding an organization's attack surface

SECURITY FEATURES

Footprinting and Reconnaissance

Quickly mapping an organisations attack surface is an essential skill for network attackers (penetration testers, bug bounty hunters or Mr Robot) as well as those who are defending the network (network security folks, system administrators, blue teams etc).

A detailed footprint of an organisations Internet facing systems is a tactical resource that can be used by both attackers and defenders. By developing an understanding of the attack surface skilled security analysts are able to quickly identify weak areas in the attack surface.

Discovered assets such as old servers, custom web applications and forgotten services are often the first crumbs in a trail that leads to a compromise.

Attack Surface Discovery is Time Critical

Penetration Testers need to quickly identify the weak spots so that they can gain access and ensure that the engagement is successful. The nature of a penetration test is time constrained so the faster areas to attack are identified the more likely the test will be a success.

Bug Bounty Hunters need to quickly identify weak spots to find the bugs and get the bounty. Since a hunter is competing against others in the race to find bugs, being faster can often mean getting paid. This is not to say that more involved deeper bug discoveries do not take time to develop, but a quick wins give you time to go for more.

Footprinting a Domain is an Iterative Process

After working through the process of footprinting a domain, you will quickly realise how it is a cyclic process. The output from searching against the domain, provides new inputs into the same domain search process. This can go on for quite some time, with both **time** and **scope** factors in the value of continuing the discovery.
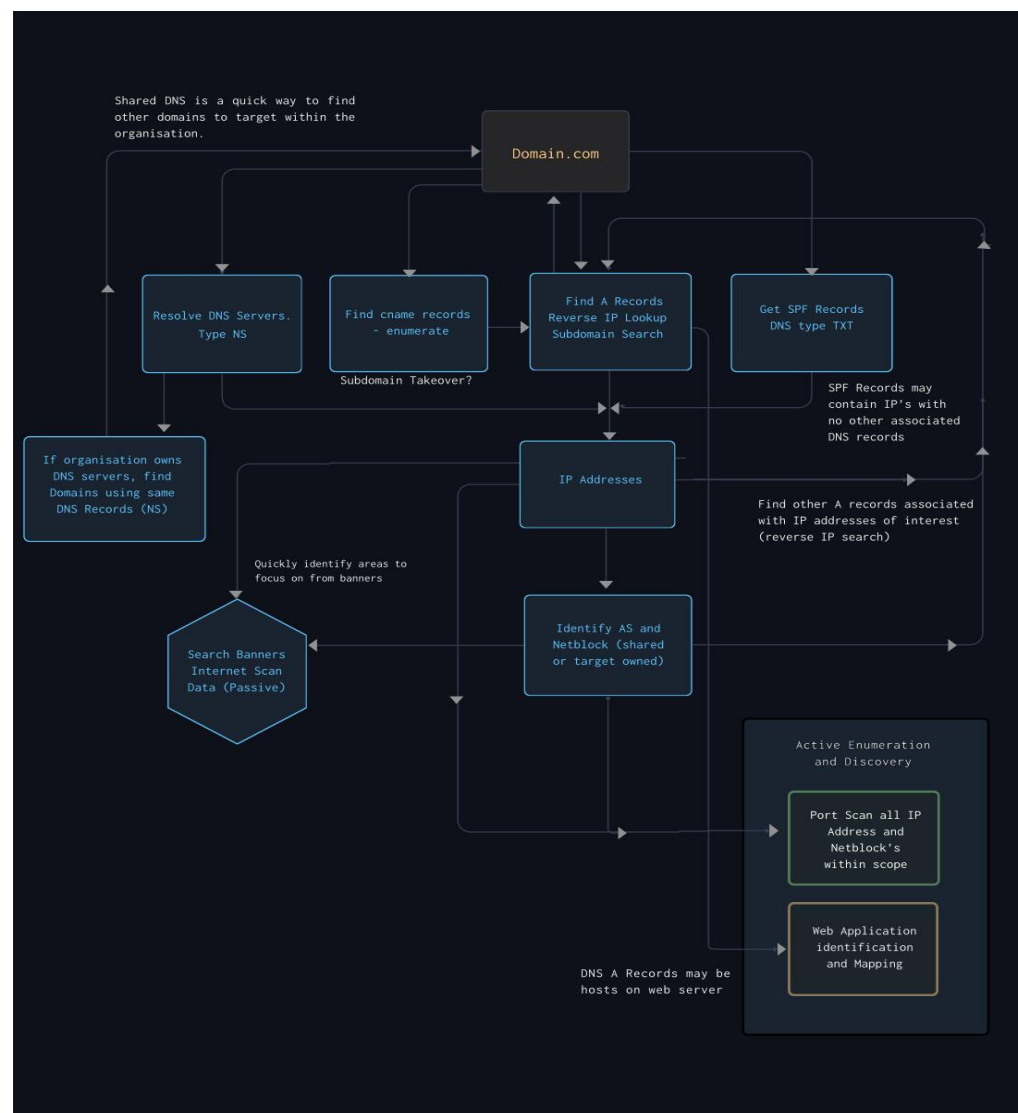

Figure 1:flow chart of footprinting a domain

METHODOLOGY

1. Go to the website: https://dnsdumpster.com/
2. Enter a domain to test (ensure that the domain is safe to use without any malicious redirects
3. The domain name I have chosen for analysation is iana.org
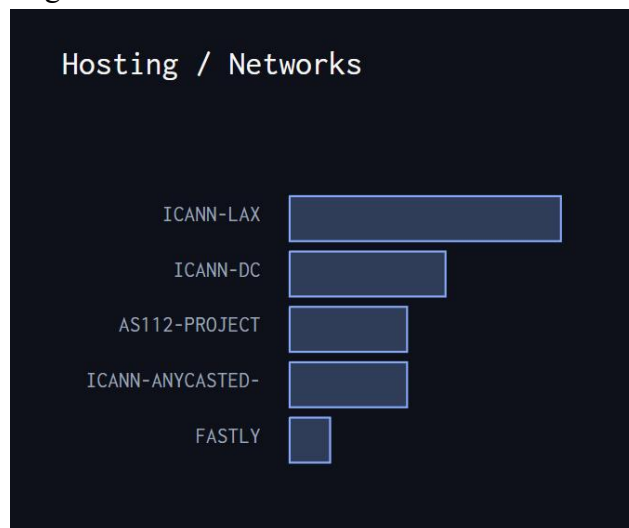4. Analyse the results

RESULTS

1.System Locations: specifies the countries wheerever this domain is available in worldmap

Figure 2 :system locations

2.Hosting Networks: **different networks / hosting providers** that are serving resoures for the iana.org.

Figure 3 :hosting

networks

ICANN-LAX

- Hosting infrastructure located in Los Angeles, managed by ICANN.

- Likely one of the primary datacenters handling DNS and web services for IANA.

ICANN-DC

- Hosting infrastructure in Washington D.C. (another ICANN data center).

- Provides redundancy and geographical distribution for resilience.

AS112-PROJECT

- A special network project (AS112) used for handling misdirected reverse DNS queries.

- It's a collaborative effort across multiple organizations to reduce unnecessary load on the root DNS system.

ICANN-ANYCASTED-

- Refers to ICANN's **anycast DNS network**, where multiple servers across the globe share the same IP addresses.

- Ensures faster response times and global availability for DNS services.

FASTLY

- A global Content Delivery Network (CDN) provider.

- Likely used by ICANN/IANA to cache and serve web content more efficiently worldwide

3.1 Services: It tells you **what kind of server software** is running on the target's IPs.Example: Apache, Nginx, GitHub Pages, FTP, etc.

3.2 Banners:A "banner" is information that a service leaks when you connect to it (like a handshake message).Example: "Apache" banner tells us the server is running Apache web server software.

Figure 4:Services/banners

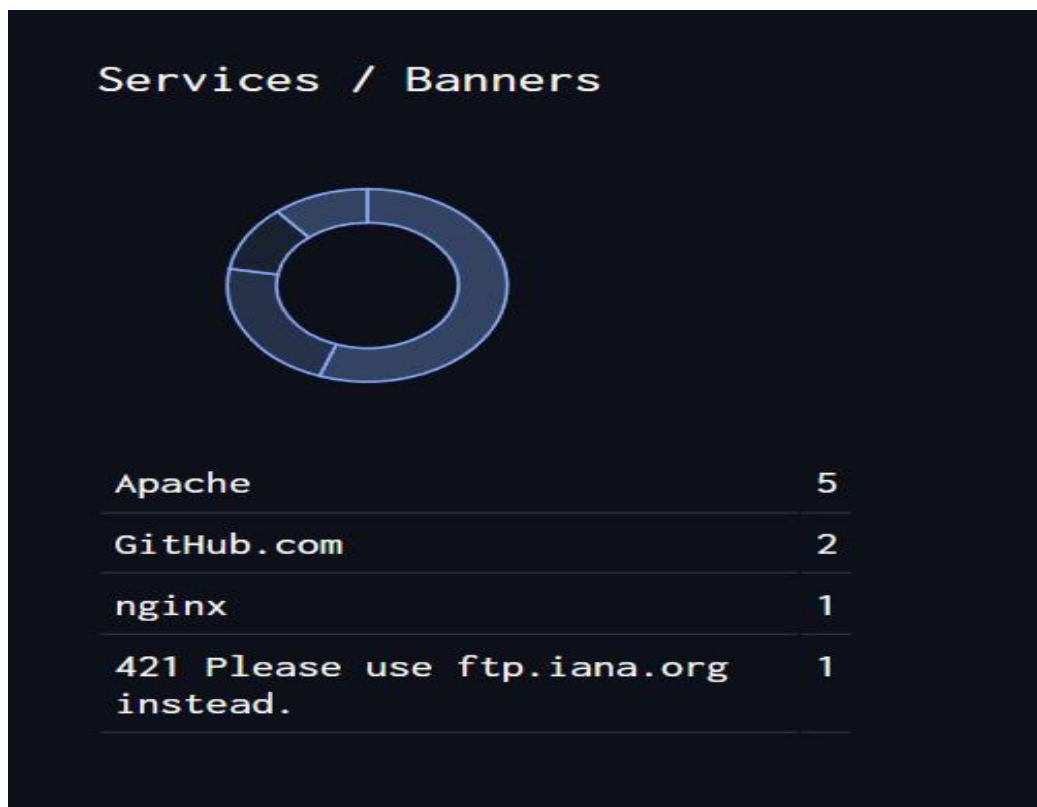**Serurity perspective :why it matters**

Attackers use service/banner info to identify software versions → which can reveal vulnerabilities.

Example: If Apache is outdated, it may have known exploits.

Defensive teams can use this data to:

- Remove banner information (banner-grabbing hardening).

- Patch/upgrade services.

- Minimize exposed services.

- Enables fingerprinting for targeted explotits

A Records (Subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)
blackhole-1.iana.org	192.175.48.6	112	AS112-PROJECT United States	8
blackhole-2.iana.org	192.175.48.42	112	AS112-PROJECT United States	6
handbook.int.iana.org	185.199.108.153	54113	FASTLY United States	http: GitHub.com, title: Site not found, tech: GitHub Pages Varnish, https: GitHub.com, title: Site not found, cn: .github.io, tech: GitHub Pages Varnish
itar.iana.org	192.0.43.12	40528	ICANN-LAX United States	http: unknown server, tech: Apache HTTP Server, https: Apache, title: 302 Found, cn: .iana.org, o: Internet Corporation For Assigned Names and Numbers, tech: Apache HTTP Server
lists.iana.org	192.0.33.32	40528	ICANN-LAX United States	https: nginx, title: 503 Service Temporarily Unavailable, cn: .iana.org, o: Internet Corporation For Assigned Names and Numbers, tech: Nginx
prisoner.iana.org	192.175.48.1	112	AS112-PROJECT United States	3

Table 1: :Address record

An A Record (Address Record) maps a domain name (like iana.org) to its IPv4 address (like 199.43.132.53).

MX Records

Priority	Host	IP	ASN	ASN Name
10	pechora6.icann.org	192.0.46.72	16876	ICANN-DC United States
10	pechora7.icann.org	192.0.33.73	40528	ICANN-LAX United States
10	pechora8.icann.org	192.0.46.74	16876	ICANN-DC United States
10	pechora1.icann.org	192.0.33.71	40528	ICANN-LAX United States

TAble 2 :MX Records

An **MX Record (Mail Exchange Record)** specifies the **mail server** responsible for receiving emails for a domain.

NS Records

Host	IP	ASN	ASN Name
c.iana-servers.net	199.43.134.53	12041	AS-AFILIAS1 United States
ns.icann.org	199.4.138.53	26710	ICANN-ANYCASTED-SERVICES United States
a.iana-servers.net	199.43.135.53	26710	ICANN-ANYCASTED-SERVICES United States
b.iana-servers.net	199.43.133.53	26710	ICANN-ANYCASTED-SERVICES United States

TAble 3 :NS Records

An **NS Record (Name Server Record)** specifies the **authoritative DNS servers** for a domain.

Purpose:

It tells the internet **which servers are responsible** for answering queries about a particular domain (like iana.org).

TXT Records

- "v=spf1 redirect=icann.org"

- "c9e864a6c53444038d34fe3a22513b74"

- "hibp-verify=dweb_deeci9b66kmruhrzqi0rgz1m"

- "docusign=b2d7c7b0-4627-494b-a7aa-682ee87c265d"

- "smartsheet-site-validation=CcnvONgQ2ibuzf2zHZxgPaWUqTwt-Sjr"

- "google-site-verification=iIqTTcUxND4wZOeVe5Ho728rH3JOSDnssYsYJ7pUtQQ"

- "MS=ms22660639"

A **TXT Record (Text Record)** is a type of DNS record that allows domain owners to store arbitrary text in the DNS.

Primarily used for **security and verification** (not for mapping domains to IPs).

SUMMARY

Domain Profiler Summary for iana.org

Generated on: 2025-08-29 17:01:50

Top 5 Banners	
Name	Count
Apache	5
GitHub.com	2
nginx	1
421 Please use ftp.iana	1

Top 5 ASN			
ASN	ASN Name	Network Range	Count
40528	ICANN-LAX	192.0.32.0/22	7
16876	ICANN-DC	192.0.44.0/22	4
112	AS112-PROJECT	192.175.48.0/24	3
26710	ICANN-ANYCASTED-SERVICES	199.43.133.0/24	3
54113	FASTLY	185.199.108.0/24	1

Top 5 Countries	
Name	Count
United States	19

OUTCOMES

Gained practical knowledge of **DNS reconnaissance** using DNSDumpster.

Learned the role of **A, MX, NS, and TXT records** in domain infrastructure.

Understood how to interpret **hosting/network information** and ASN details.

Acquired skills to analyze **services and banners** for potential vulnerabilities.

Realized the importance of **DNS footprinting** in penetration testing and OSINT.

Developed awareness of **security best practices** like minimizing exposed services, hardening banners, and securing DNS configurations.

CONCLUSION

The DNSDumpster tool provided valuable insights into the DNS infrastructure of iana.org . The analysis revealed various A records, MX records, NS records, and TXT records, along with associated hosting networks and open services. This information is crucial for understanding the domain's attack surface and can be used for security assessments, threat analysis, and network management. The tool effectively consolidates publicly available DNS information, making it a powerful resource for reconnaissance and research in cybersecurity
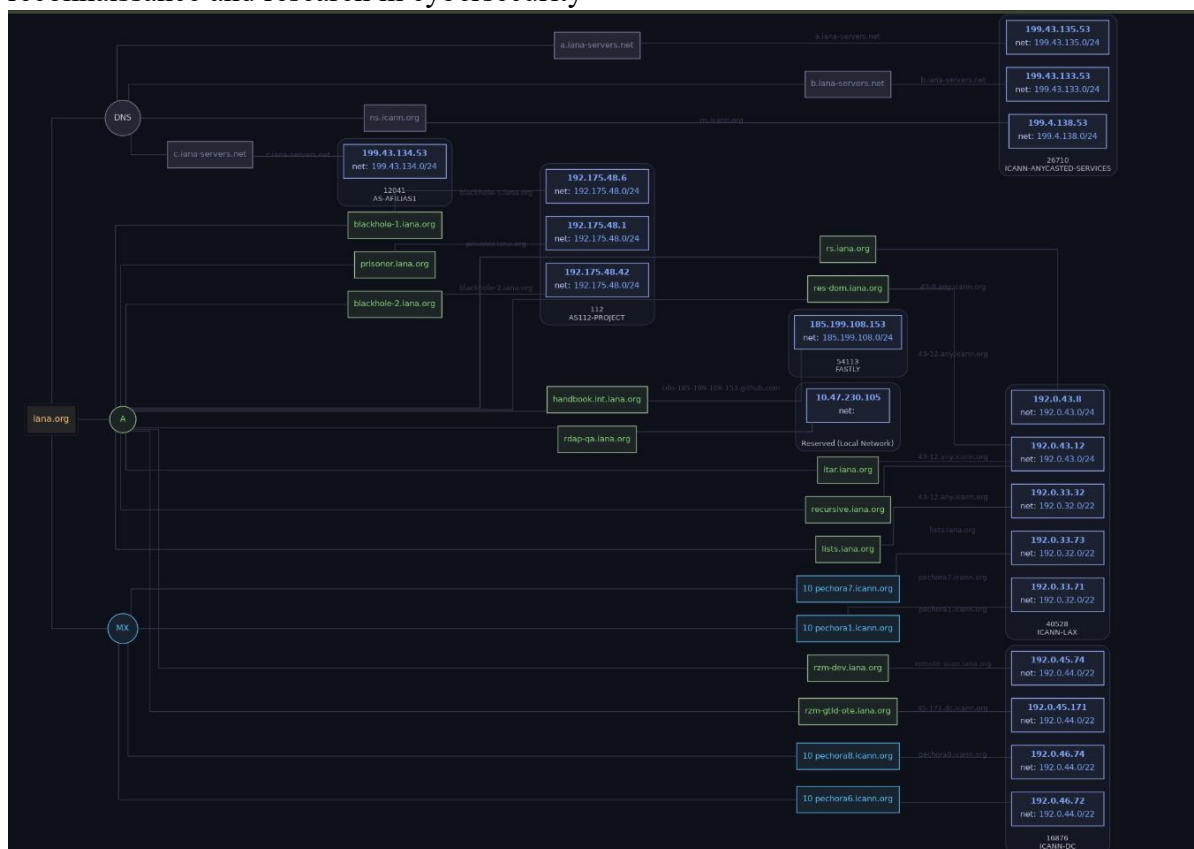

figure 5: Map for the footprint fot domain