FootPrinting on https://www.kayak.co.in/

Abstract

Footprinting is the foundational phase of ethical hacking, focused on gathering publicly accessible information about a target system without direct interaction or intrusion. This report presents a systematic footprinting analysis of the travel website kayak.co.in, using tools and techniques such as IP geolocation, DNS enumeration, WHOIS lookup, and service banner identification. The objective is to understand the site's hosting infrastructure, network distribution, and potential exposure points. Findings reveal a globally distributed architecture hosted by Fastly Inc., with multiple IP addresses across India, the Netherlands, and the United States. The report also highlights SSL certificate anomalies and redirect behavior, suggesting the use of CDN and proxy routing. These insights lay the groundwork for deeper security assessments in later phases of ethical hacking.

Introduction

In the realm of cybersecurity, footprinting serves as the reconnaissance stage where ethical hackers collect detailed information about a target system to assess its security posture. This passive data collection is crucial for mapping the digital surface of a website or network without triggering defensive mechanisms. The target of this analysis is kayak.co.in, a travel booking platform with global reach and complex infrastructure.

The purpose of this project is to:

- Identify and document the domain’s IP addresses and geolocation
- Analyze DNS records, hosting details, and SSL certificate configurations
- Examine open ports and service banners for potential exposure
- Evaluate the site's network architecture and distribution

By applying footprinting techniques ethically and systematically, this report aims to demonstrate how publicly available data can reveal critical insights into a system’s structure and potential vulnerabilities. The findings contribute to a broader understanding of reconnaissance strategies in cybersecurity and highlight the importance of secure configurations in public-facing web services.

Let me know if you'd like help drafting the **Literature Review**, **Methodology**, or **Conclusion** next—or if you want this turned into a slide deck for presentation. I can also help you add citations or visuals if needed.

Target Overview

- **Target Domain**: https://www.kayak.co.in
- **Hosting Company**: Fastly Inc.
- **Netblock Owner**: Fastly Inc.
- **Hosting Country**: United States

- **IPv4 Address**: 151.101.157.29
- **IPv6 Address**: 2a04:4e42:25::285
- **Reverse DNS**: Unknown

DNS and Domain Information

- **Domain Registrar**: nixiregistry.in
- **Top-Level Domain**: .co.in (India)
- **Nameservers**:
  - blue.foundationdns.com
  - whois.cloudflare.com
- **DNS Admin Contact**: dns@cloudflare.com
- **Organization**: Kayak Software Corporation, United States
- **DNS Security Extensions**: Enabled

IP Address Details

🔻 Primary Hostname

- **Hostname**: dualstack.kayak.map.fastly.net
- **IPv4**: 151.101.157.29
- **IPv6**: 2a04:4e42:25::285

Geolocation of IPs

IP Address	Country	State	City	ISP
2401:4900:88b8:fd45:1655:b9ff:fe34:17c0	India	Madhya Pradesh	Gwalior	Bharti Airtel Ltd.
2404:a800:1a00:808::9 (and variants)	India	Delhi	Delhi	Bharti Airtel Ltd.
2a04:4e42:5a::285	Netherlands	Noord-Holland	Amsterdam	Fastly Inc.
151.101.157.29	United States	California	San Francisco	Fastly Inc.
199.232.25.29	United States	California	San Francisco	Fastly Inc.

ASN and Network Details

- **ASN**: AS54113 – Fastly Inc.
- **NetRange**: 151.101.0.0 – 151.101.255.255
- **CIDR**: 151.101.0.0/16
- **NetName**: SKYCA-3
- **Abuse Contact**: abuse@fastly.com
- **Tech/Admin/NOC Contact**: Fastly RIR Administrator (+1-415-404-9374)
- **Organization Address**: PO Box 78266, San Francisco, CA 94107, US

SSL Certificate Details

Issued By: DigiCert Global €3 TLS ECC SHA384 2020 CAI

Issued To: w»u.ihg.com (Six Continents Hotels, Inc.)

Supported Versions: TLSv1.2, TLSv1.3

HTTP Response Headers

◆ Forbidden Access

HTTP/1.1 403 Forbidden Content-Type: text/html Set-Cookie: akamaiCountryCode=US; path=/; secure; SameSite=Strict

◆ Redirect

HTTP/1.1 301 Moved Permanently Location: https://www.oracle.com/corporate/acquisitions/next-technik/

🔍 Open Ports and Services

Port	Count
443 (HTTPS)	8
80 (HTTP)	6

◆ Service Banners

- **HTTP**: Varnish (Fastly error: unknown domain)
- **HTTPS**: Unknown server
- **Common Name**: www.kayak.com

□ Analysis & Observations

- The domain is hosted by Fastly Inc., a CDN provider, indicating high availability and global distribution.
- Multiple IPs across India, Netherlands, and the US suggest load balancing and edge server deployment.
- SSL certificate mismatch may be due to shared infrastructure or proxy routing.
- DNSSEC is enabled, improving domain-level security.
- Open ports 80 and 443 are standard, with Varnish caching observed—common in CDN setups.

✅ Conclusion

This footprinting exercise reveals that kayak.co.in is a globally distributed web service hosted via Fastly CDN. The infrastructure is robust, with multiple IPs and geographic redundancy. While no direct vulnerabilities were found, the SSL certificate configuration and redirect behavior warrant further investigation in a penetration testing phase.

Tools used:

- ipinfo.io
- whois.domaintools.com
- sitereport.netcraft.com
- www.shodan.io
- Dnsdumpster.com