Report Format

Title: Information Gathering Report for senselearner.com

Date: 16-09-23

Prepared by: Saba Perveen **Position:** Intern

Objective:

The objective of this report is to present the findings of the information gathering and reconnaissance activities conducted on senselearner.com in a legal and ethical manner. The information collected is intended for security assessment and risk analysis.

Executive Summary

In our investigation of senselearner.com, we uncovered significant details related to its domain, DNS records, web server, network, WHOIS data, open-source intelligence, vulnerabilities, and security concerns. Our report highlights the key findings to assist in making informed security decisions. provide a brief overview of the key findings and highlights of your information gathering efforts. The DNS foot-printing for senselearner.com reveals several key findings. The domain is registered with senselearner.com and has been active since August 7, 2019. The DNS records show the domain's primary IP address as 162.250.126.19, and it has MX records associated with Google's email services. The domain also has TXT records for SPF and Google site verification. In terms of subdomains and associated services, the report does not provide specific information on subdomains or services linked to DNS records. Metadata from web pages is not included. Regarding network and WHOIS enumeration, the WHOIS records indicate that the domain is associated with Senselearner Technologies Private Limited, a Private Limited Indian Non-Government Company registered on August 7, 2019. It is unlisted, and additional company details are provided, including the CIN/LLPIN/FCRN, date of AGM, and ROC Code.

Table of Contents

Introduction

Our investigation was initiated to evaluate the security status of senselearner.com, considering potential risks and vulnerabilities. We aim to provide comprehensive insights to support security decisions

Domain Information

- Domain Name: senselearner.com
- IP Address: 162.250.126.19
- Registrar: senselearner.com
- Registration Date: 07 August 2019
- Status: Active

DNS Footprinting

Summarize the findings from DNS footprinting, including:

- **List of DNS Records:**

  Name: senselearner.com

  - TTL: 5486
  - IP: 162.250.126.19

MX Records:

- Name: senselearner.com
    - TTL: 14400
    - IP: 142.250.153.27
    - MX: ALT4.ASPMX.L.GOOGLE.com.
    - Preference: 10
- Name: senselearner.com
    - TTL: 14400
    - IP: 142.250.27.26
    - MX: ALT3.ASPMX.L.GOOGLE.com.
    - Preference: 10
- Name: senselearner.com
    - TTL: 14400
    - IP: 74.125.193.26
    - MX: ALT1.ASPMX.L.GOOGLE.com.
    - Preference: 5
- Name: senselearner.com
    - TTL: 14400
    - IP: 64.233.184.27
    - MX: ALT2.ASPMX.L.GOOGLE.com.
    - Preference: 5
- Name: senselearner.com
    - TTL: 14400
    - IP: 142.251.167.26
    - MX: ASPMX.L.GOOGLE.com.

    - Preference: 1

NS Records:

- Name: senselearner.com
    - TTL: 8355
    - Value: dns2014b.trouble-free.net.
- Name: senselearner.com
    - TTL: 8355
    - Value: dns2014a.trouble-free.net.

SOA Records:

- Name: senselearner.com
    - TTL: 21600
    - Mname: dns2014a.trouble-free.net.
    - Rname: not-monitored-email.interserver.net.

TXT Records:

- Name: senselearner.com
    - TTL: "14400"
    - Value: "v=spf1 +a +mx +ip4:162.250.126.18 include:relay.is.cc ~all"
- Name: senselearner.com
    - TTL: "21600"
    - Value:"google-site-verification=21dWAeLOTAQNSrIU2i9YzlB0tIKGG9XWbI5XunkOx10"

- **Subdomains:** Enumerate any subdomains discovered.
- **Associated Services:** Identify any services or applications linked to DNS records.

Web Footprinting

Detail the results of web footprinting, such as:

- **Web Server Information:** Identify the web server software and version.
- **Directory and File Structure:** Document any directories or files discovered.
- **Technologies in Use:** List content management systems (CMS), frameworks, or scripting languages used.
- **Metadata:** Include metadata from web pages, if available.

Network and WHOIS Enumeration

Discuss network and WHOIS enumeration results:

- **Network Range:** Note the network range and IP addresses.
- **WHOIS Records:**

The WHOIS records for senselearner.com are as follows:

- Company Name: Senselearner Technologies Private Limited
- Additional Director: Sneha
- CIN/LLPIN/FCRN: U72900UP2019PTC119946
- Company Classification: Private Limited Indian Non-Government Company
- Incorporation Date: 07 Aug 2019
- Date of AGM: 31 Dec 2020
- Date of Balance Sheet: 31 Mar 2020
- Listing Status: Unlisted
- ROC Code: Roc-Kanpu

Open-Source Intelligence (OSINT)

Senselearner is an active domain registered with senselearner.com since August 2019. DNS footprinting reveals its primary IP address and MX records connected to Google's email services. Subdomains and associated services are not specified. Web footprinting details, including web server software, directory structure, technologies, and metadata, are absent from the provided information. In terms of network and WHOIS enumeration, the domain is associated with

Senselearner Technologies Private Limited, a Private Limited Indian Non-Government Company registered in August 2019. It remains unlisted, and specific ASN information is not available.

Vulnerabilities and Security Concerns

Presence of MX records linked to Google's email services suggests a level of email security provided by Google. It's important to regularly update and patch any web servers and software used, maintain strong access controls, and monitor for suspicious activities to mitigate potential security risks. Further analysis and testing would be required to identify any specific vulnerabilities or security issues on the website.

Recommendations

Provide recommendations for addressing any identified vulnerabilities or concerns.

These recommendations may include:

- Updating software or patches.
- Enhancing server security configurations.
- Securing sensitive information.
- Implementing best practices for online privacy.

Conclusion

In conclusion, senselearner.com is an active domain registered since August 2019, associated with Senselearner Technologies Private Limited. DNS footprinting reveals its IP address and MX records connected to Google's email services, while web footprinting details, such as server software and technology, are not provided. While specific vulnerabilities or security concerns aren't evident from the data, ongoing security best practices are essential to safeguard the domain.

Appendices

These supplementary details offer a comprehensive overview of the domain's registration, DNS configuration, and associated company information. While specific web server software, directory structures, and potential security concerns aren't covered extensively in the main report, the appendices provide a more in-depth resource for those seeking detailed technical insights into the domain's infrastructure and ownership.

References

https://www.thecompanycheck.com/company/senselearner-technologies-private-limited/U72900UP2019PTC119946
https://senselearner.com/
https://www.instagram.com/senselearner_technologies/
https://twitter.com/senselearnerl
https://www.linkedin.com/company/senselearner-technologies-pvt-ltd/
https://www.facebook.com/senselearner/