Information Gathering

Report for senselearner.com

Date: - 27-Sept-2023

Name: - Onkar vikas mhaskar

Role: - Cyber Security 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

This executive summary provides a concise overview of the findings and recommendations outlined in the comprehensive cybersecurity assessment report. The assessment focused on evaluating the digital presence and security posture of the target organization through various information gathering techniques and vulnerability identification. The primary goal was to identify potential security vulnerabilities and provide actionable recommendations to strengthen the organization's cybersecurity defenses.

Table of Contents:

Introduction

Purpose of the Report:

This report is prepared to document the results of an information gathering process conducted within the context of a cybersecurity assessment. The information gathering exercise was initiated to comprehensively analyze and assess the security posture of a specific target entity. This report outlines the reasons behind this undertaking, presents the objectives set for the information gathering, and provides a structured overview of the findings and recommendations.

Context of the Information Gathering:

The information gathering was conducted in the context of a broader cybersecurity assessment aimed at enhancing the digital security of the target organization. As cyber threats continue to evolve and pose significant risks to businesses and institutions, proactive measures are crucial to safeguard sensitive data, infrastructure, and operations. The assessment focused on gathering essential data and intelligence related to the organization's digital presence, vulnerabilities, and potential security gaps.

Reasons for Task Assignment:

The assignment of this task was prompted by the growing importance of cybersecurity in today's interconnected world. As cyber threats become more sophisticated and prevalent, organizations recognize the need to proactively assess their vulnerabilities and strengthen their defenses. The assignment was made with the following key considerations in mind:

1.Risk Mitigation: To identify and mitigate potential security risks and vulnerabilities that could expose the organization to cyberattacks.

2.Compliance Requirements: To ensure compliance with industry-specific regulations and best practices related to information security.

3.Data Protection: To safeguard sensitive data, including customer information, intellectual property, and confidential business data.

Objectives of the Information Gathering:

The primary objectives of the information gathering process were as follows:

1.Domain Information: To collect comprehensive data about the organization's digital presence, including domain names, subdomains, and associated IP addresses.

2.DNS Footprinting: To analyze the Domain Name System (DNS) to identify potential vulnerabilities, misconfigurations, and information leakage.

3.Web Footprinting: To gain insights into the web applications, web servers, and content hosted by the organization, including identifying open ports and services.

4.Network and WHOIS Enumeration: To enumerate network infrastructure, analyze WHOIS data, and understand the organization's network topology.

5. Open-Source Intelligence (OSINT): To leverage publicly available information and intelligence sources to gather insights about the organization's online presence, personnel, and potential security weaknesses.

6.Vulnerabilities and Security Concerns: To identify vulnerabilities, security concerns, and potential attack vectors that could be exploited by malicious actors.

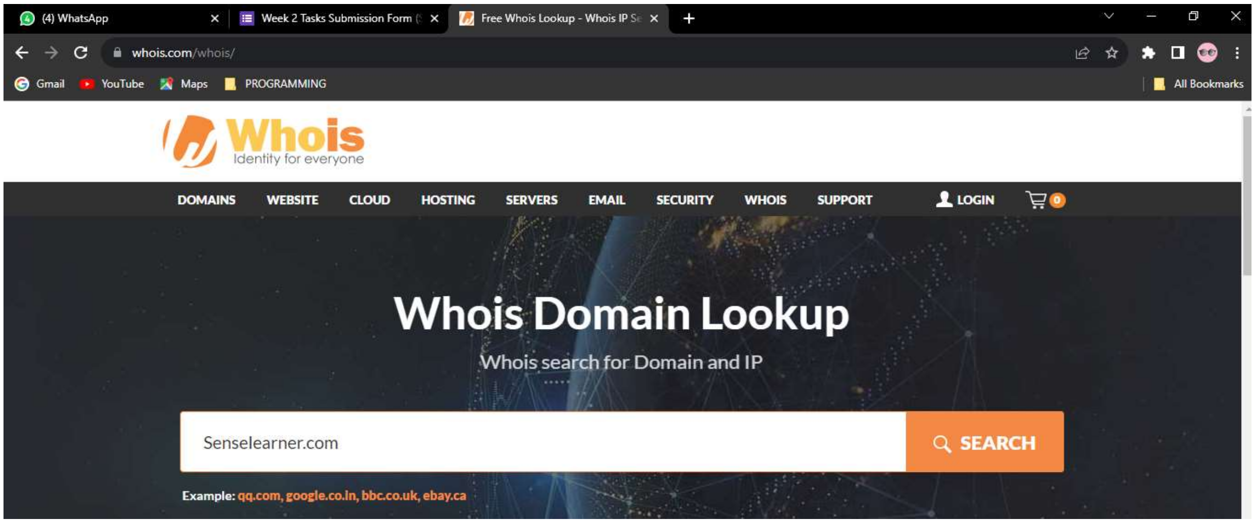
7.Recommendations: To provide actionable recommendations and best practices for improving the organization's cybersecurity posture.

8.Conclusion: To summarize the findings, key takeaways, and the overall state of the organization's security.

The following sections of this report will delve into each of these objectives, providing detailed findings and recommendations to support the overarching goal of enhancing the organization's cybersecurity defenses.

Whois Domain Tool

This is a database that contains information about registered domain names. A WHOIS lookup can help you identify the domain name of a company and provide information about the domain's owner, registration date, and expiration date, Status, Registrant and Administrative contact number .



Whois Domain Lookup

Whois search for Domain and IP

Senselearner.com

Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

Domain Information

Domain Name: senselearner.com

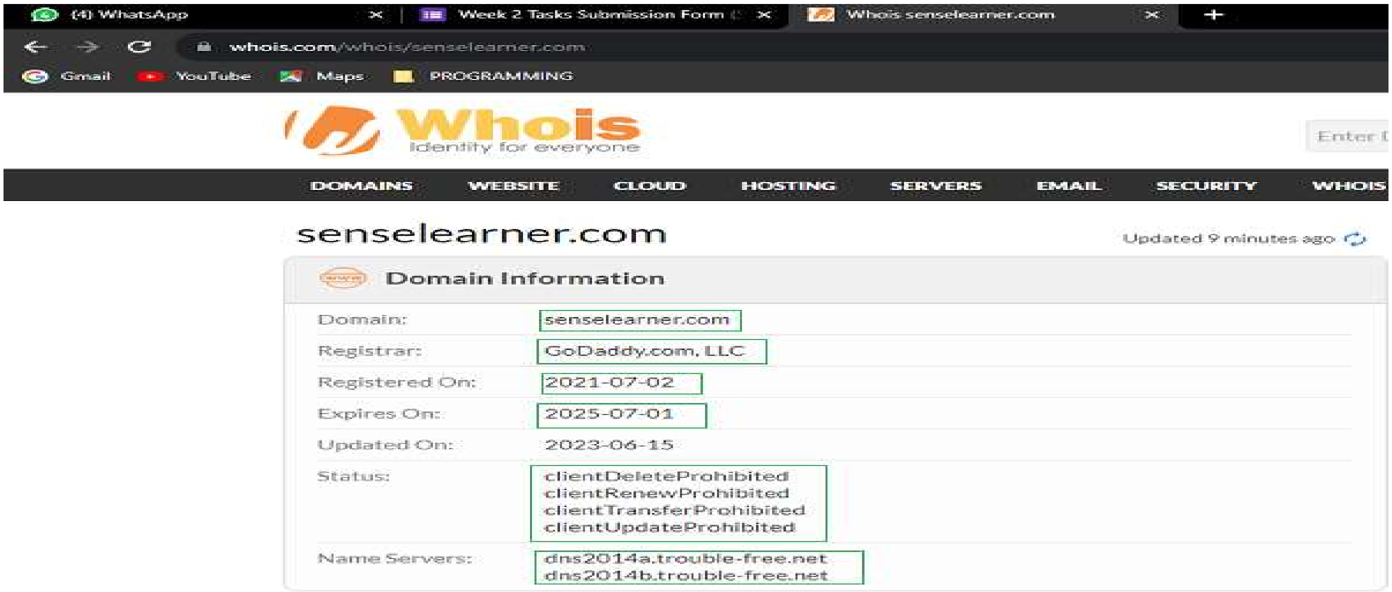
IP Address: 162.250.126.19

Registrar: GoDaddy.com, LLC, IANA ID: 146

Registration Date: 02-07-2021

Expiry Date: 01-07-2025

Status: clientDeleteProhibited
clientRenewProhibited
clientTransferProhibited
clientUpdateProhibited



senselearner.com

Domain Information

Domain:	senselearner.com
Registrar:	GoDaddy.com, LLC
Registered On:	2021-07-02
Expires On:	2025-07-01
Updated On:	2023-06-15
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	dns2014a.trouble-free.net dns2014b.trouble-free.net

DNS Footprinting

CentralOps.net

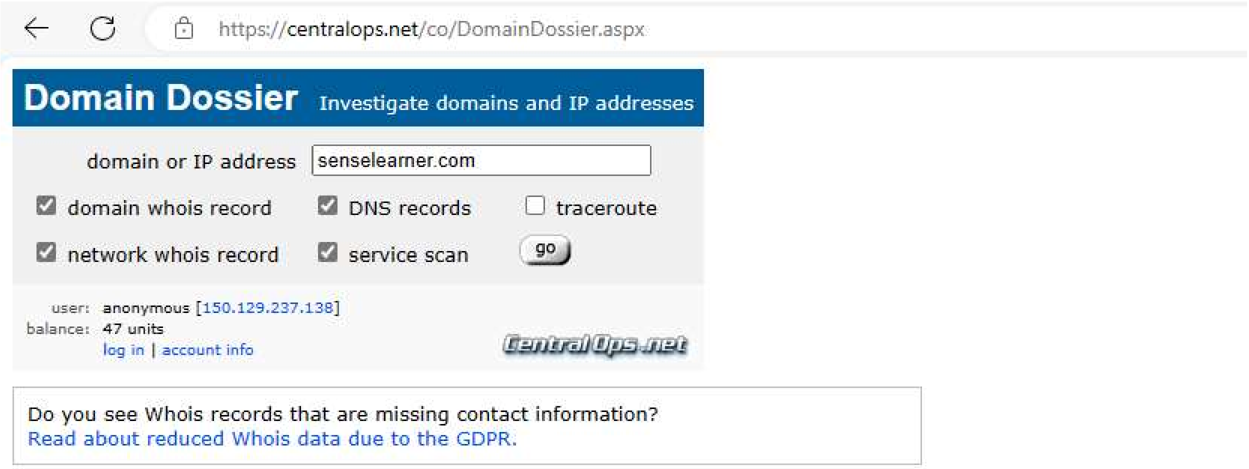
It is a website that provides free online network tools such as traceroute, nslookup, dig, whois lookup, ping, Domain Dossier, and Email Dossier. This tool helps to solve problems, investigate cybercrime or good understand how things are set up.

For instance, **Domain Dossier** generates reports from public records about domain names and IP addresses to provide information such as owner’s contact information, registrar and registry information, the company that is hosting a website, where an IP address is geographically located, what type of server is at the address, and the upstream networks of a site .

The other tools available on CentralOps include:

- **Traceroute**: traces the network path from one server to another.

- **NsLookup**: It looks up various domain resource records with this version of the classic NsLookup utility.
- **AutoWhois**: gets Whois records automatically for domains worldwide.
- **Email Dossier**: validates and troubleshoots email addresses.
- **Browser Mirror**: shows what your browser reveals about you.
- **Ping**: checks if a host is reachable.
- **Service scan**: scans a host for open ports.



Domain Dossier Investigate domains and IP addresses

domain or IP address: senselearner.com

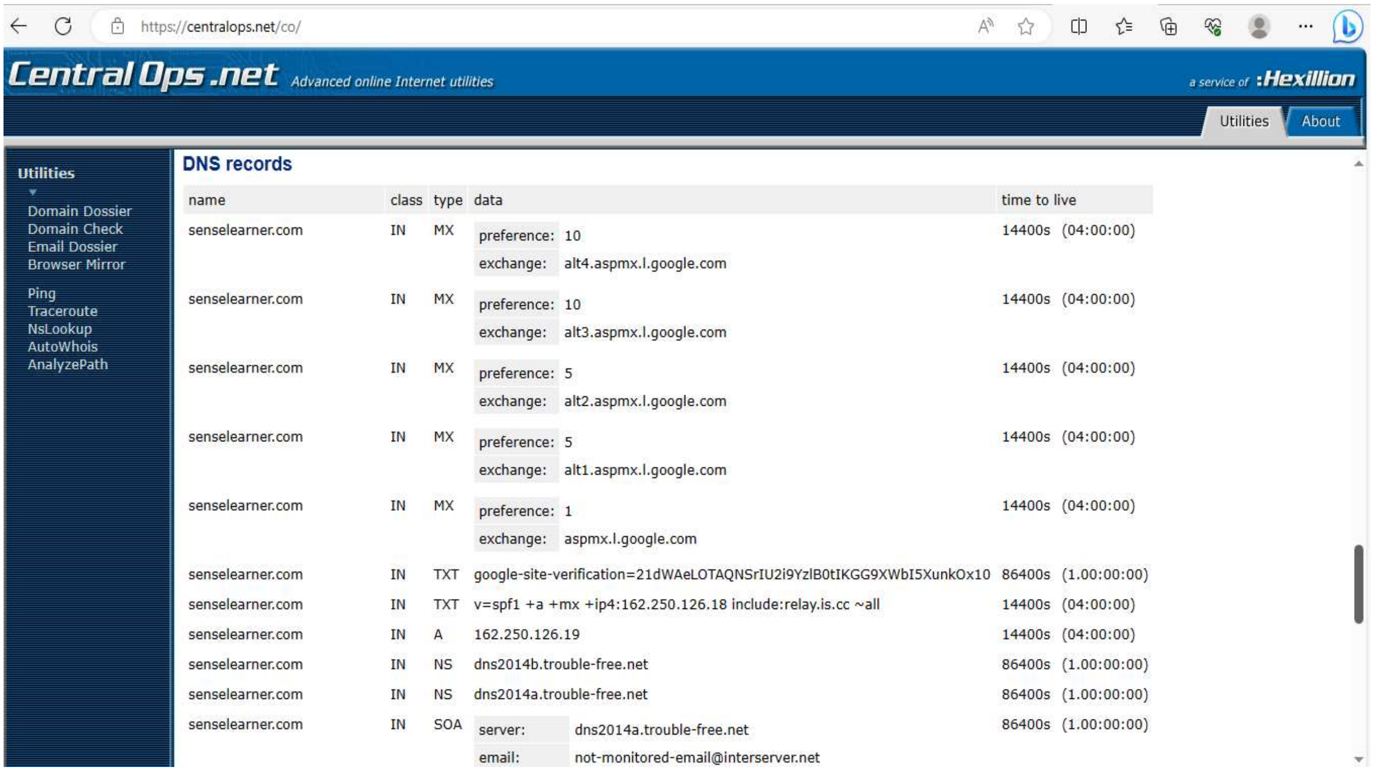
☑ domain whois record ☑ DNS records □ traceroute

☑ network whois record ☑ service scan go

user: anonymous [150.129.237.138]
balance: 47 units
log in | account info

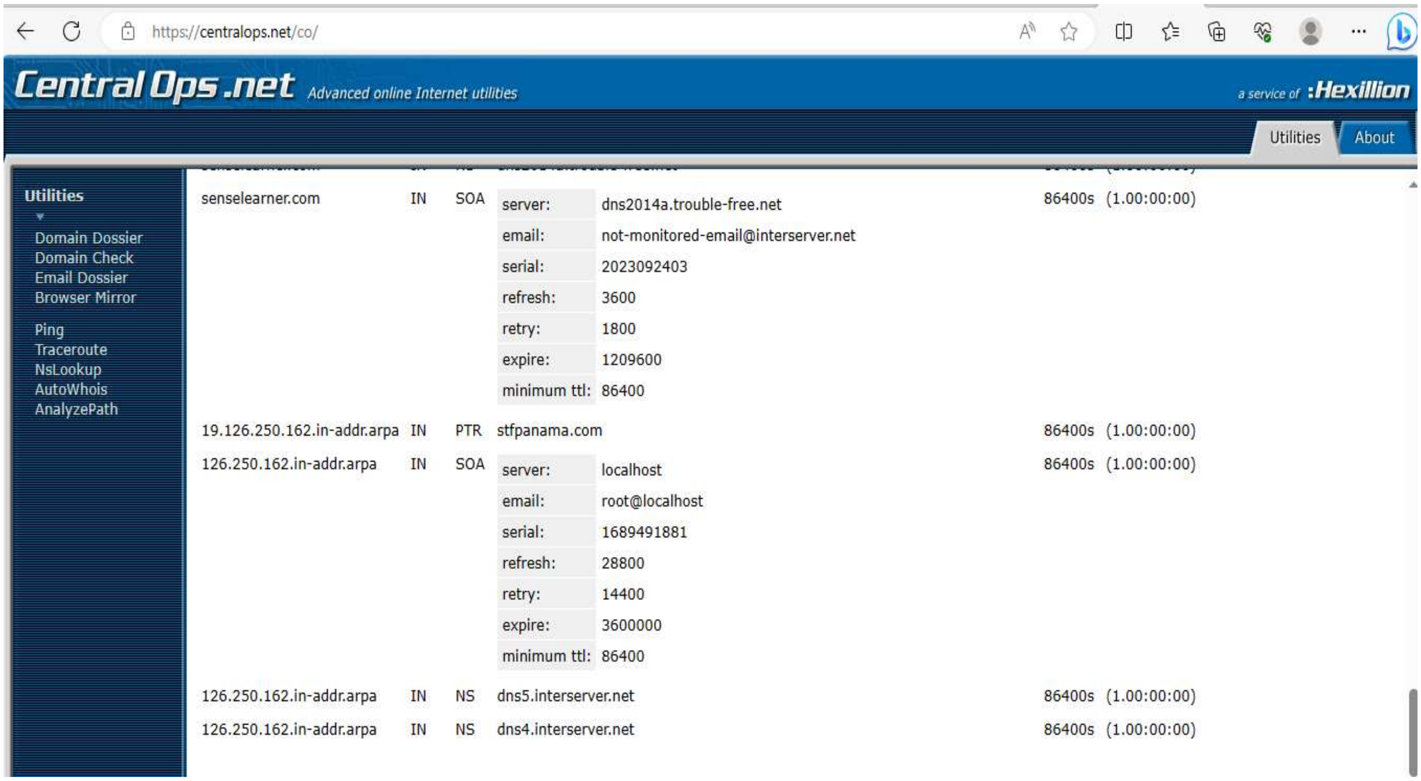
Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

List of DNS Records: Provide information on A records, MX records, CNAME records, etc.

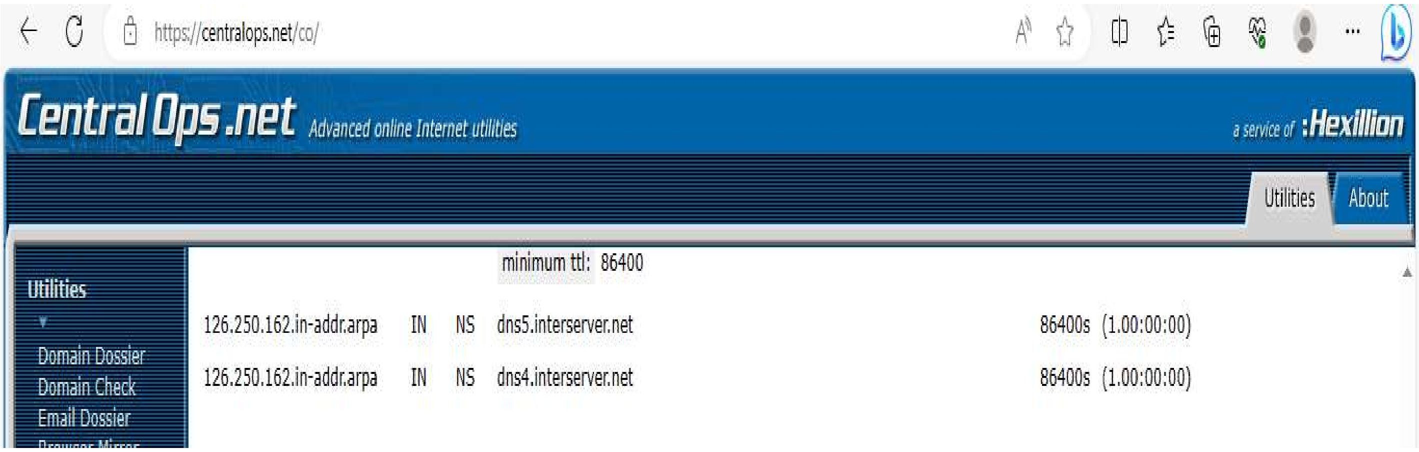


DNS records

name	class	type	data	time to live
senselearner.com	IN	MX	preference: 10 exchange: alt4.aspmx.l.google.com	14400s (04:00:00)
senselearner.com	IN	MX	preference: 10 exchange: alt3.aspmx.l.google.com	14400s (04:00:00)
senselearner.com	IN	MX	preference: 5 exchange: alt2.aspmx.l.google.com	14400s (04:00:00)
senselearner.com	IN	MX	preference: 5 exchange: alt1.aspmx.l.google.com	14400s (04:00:00)
senselearner.com	IN	MX	preference: 1 exchange: aspmx.l.google.com	14400s (04:00:00)
senselearner.com	IN	TXT	google-site-verification=21dWAeLOTAQNSrIU2i9YzlB0tIKGG9XWbI5XunkOx10	86400s (1.00:00:00)
senselearner.com	IN	TXT	v=spf1 +a +mx +ip4:162.250.126.18 include:relay.is.cc ~all	14400s (04:00:00)
senselearner.com	IN	A	162.250.126.19	14400s (04:00:00)
senselearner.com	IN	NS	dns2014b.trouble-free.net	86400s (1.00:00:00)
senselearner.com	IN	NS	dns2014a.trouble-free.net	86400s (1.00:00:00)
senselearner.com	IN	SOA	server: dns2014a.trouble-free.net email: not-monitored-email@interserver.net	86400s (1.00:00:00)

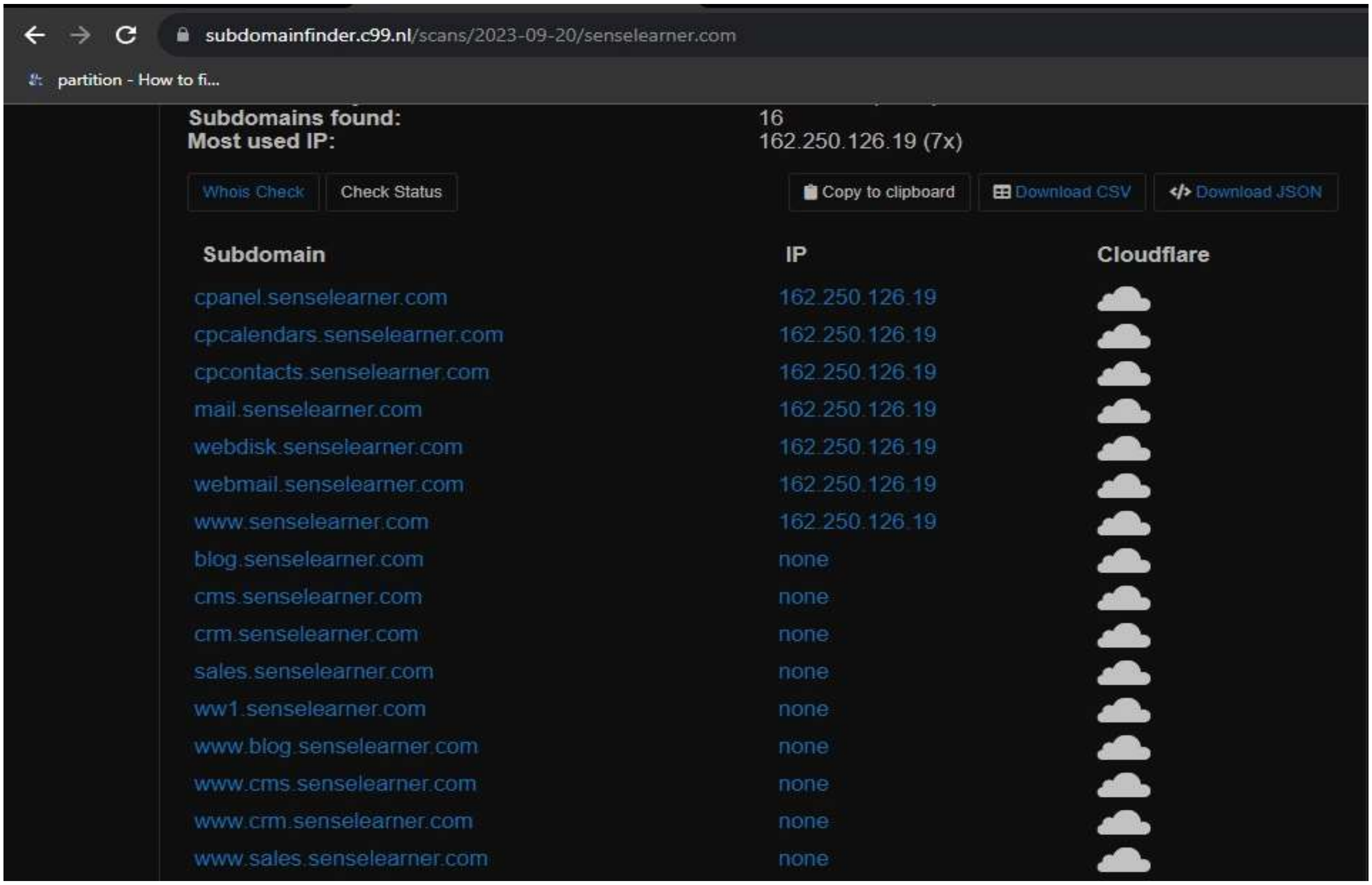


```
senselearner.com             IN   SOA   server:        dns2014a.trouble-free.net              86400s  (1.00:00:00)
                                        email:         not-monitored-email@interserver.net
                                        serial:        2023092403
                                        refresh:       3600
                                        retry:         1800
                                        expire:        1209600
                                        minimum ttl:   86400
19.126.250.162.in-addr.arpa  IN   PTR   stfpanama.com                                         86400s  (1.00:00:00)
126.250.162.in-addr.arpa     IN   SOA   server:        localhost                              86400s  (1.00:00:00)
                                        email:         root@localhost
                                        serial:        1689491881
                                        refresh:       28800
                                        retry:         14400
                                        expire:        3600000
                                        minimum ttl:   86400
126.250.162.in-addr.arpa     IN   NS    dns5.interserver.net                                  86400s  (1.00:00:00)
126.250.162.in-addr.arpa     IN   NS    dns4.interserver.net                                  86400s  (1.00:00:00)
```



```
                                        minimum ttl:   86400
126.250.162.in-addr.arpa     IN   NS    dns5.interserver.net                                  86400s  (1.00:00:00)
126.250.162.in-addr.arpa     IN   NS    dns4.interserver.net                                  86400s  (1.00:00:00)
```

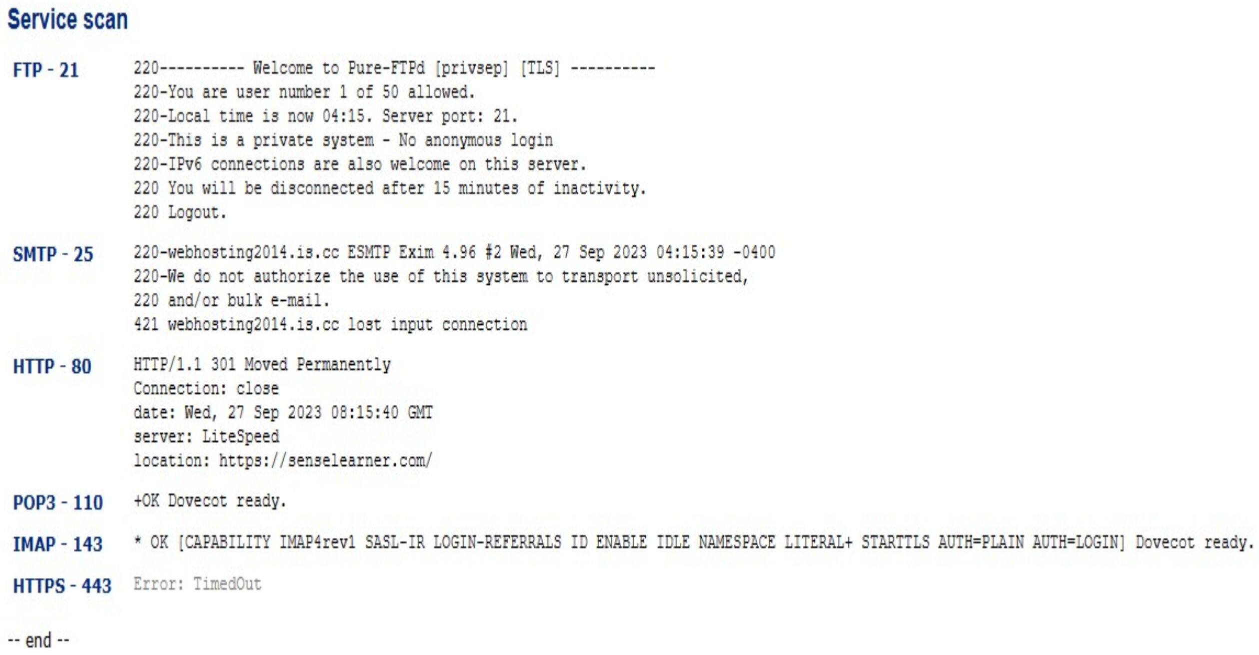
Subdomains: We find the subdomains and it’s total 16 subdomain.



Subdomains found: 16
Most used IP: 162.250.126.19 (7x)

Subdomain	IP	Cloudflare
cpanel.senselearner.com	162.250.126.19	☁
cpcalendars.senselearner.com	162.250.126.19	☁
cpcontacts.senselearner.com	162.250.126.19	☁
mail.senselearner.com	162.250.126.19	☁
webdisk.senselearner.com	162.250.126.19	☁
webmail.senselearner.com	162.250.126.19	☁
www.senselearner.com	162.250.126.19	☁
blog.senselearner.com	none	☁
cms.senselearner.com	none	☁
crm.senselearner.com	none	☁
sales.senselearner.com	none	☁
ww1.senselearner.com	none	☁
www.blog.senselearner.com	none	☁
www.cms.senselearner.com	none	☁
www.crm.senselearner.com	none	☁
www.sales.senselearner.com	none	☁

Associated Services: Identified DNS Services are FTP, SMTP, HTTP, POP3, IMAP, HTTPS.



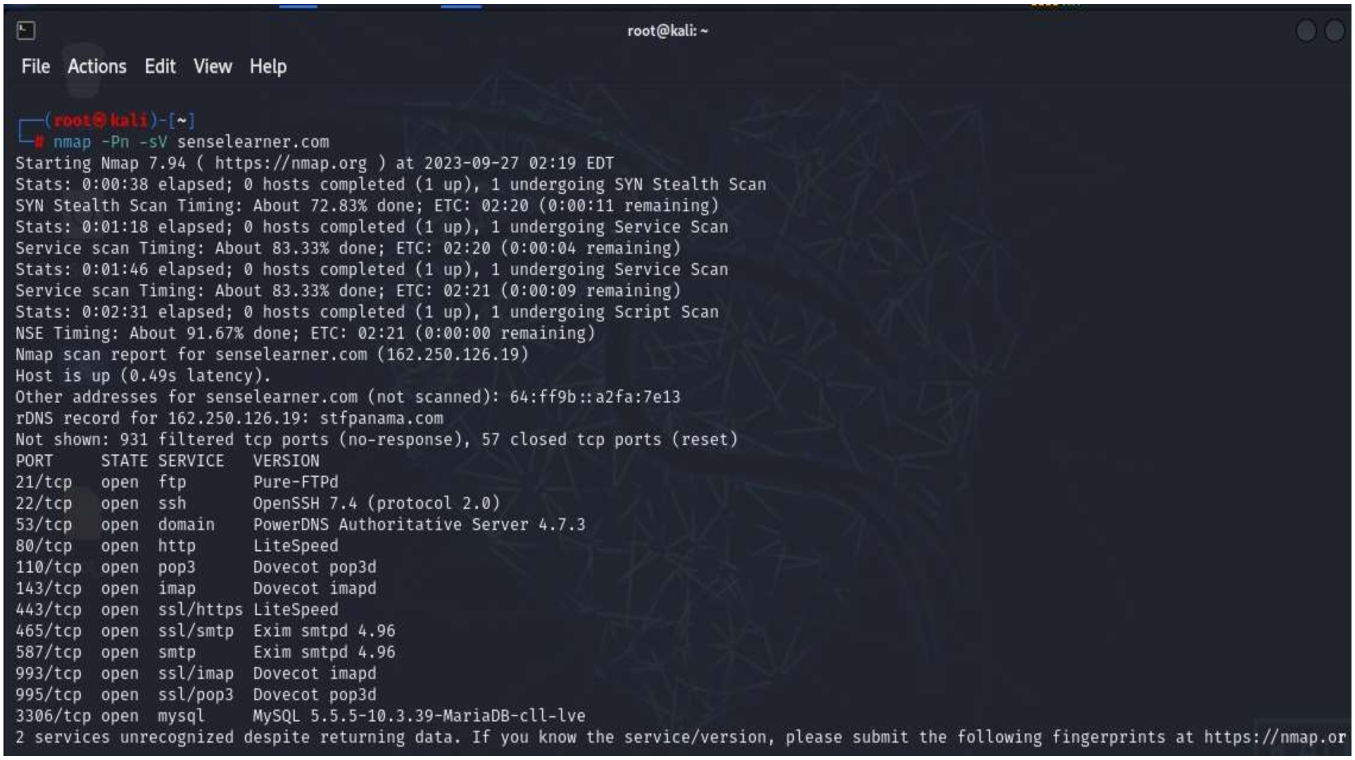
Service scan

```
FTP - 21      220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
              220-You are user number 1 of 50 allowed.
              220-Local time is now 04:15. Server port: 21.
              220-This is a private system - No anonymous login
              220-IPv6 connections are also welcome on this server.
              220 You will be disconnected after 15 minutes of inactivity.
              220 Logout.

SMTP - 25     220-webhosting2014.is.cc ESMTP Exim 4.96 #2 Wed, 27 Sep 2023 04:15:39 -0400
              220-We do not authorize the use of this system to transport unsolicited,
              220 and/or bulk e-mail.
              421 webhosting2014.is.cc lost input connection

HTTP - 80     HTTP/1.1 301 Moved Permanently
              Connection: close
              date: Wed, 27 Sep 2023 08:15:40 GMT
              server: LiteSpeed
              location: https://senselearner.com/

POP3 - 110    +OK Dovecot ready.

IMAP - 143    * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.

HTTPS - 443   Error: TimedOut
```

-- end --

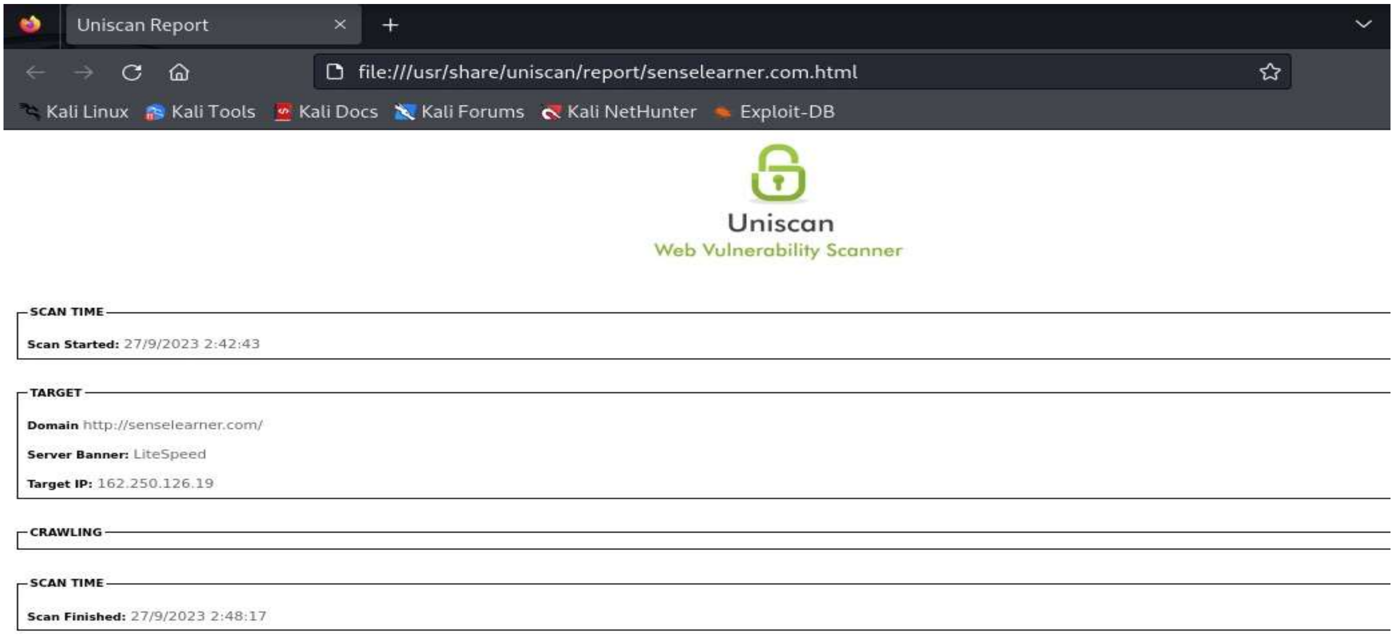
Web Footprinting

Web Server Information: Identify the web server software and version.



```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sV senselearner.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-27 02:19 EDT
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 72.83% done; ETC: 02:20 (0:00:11 remaining)
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 02:20 (0:00:04 remaining)
Stats: 0:01:46 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 02:21 (0:00:09 remaining)
Stats: 0:02:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 91.67% done; ETC: 02:21 (0:00:00 remaining)
Nmap scan report for senselearner.com (162.250.126.19)
Host is up (0.49s latency).
Other addresses for senselearner.com (not scanned): 64:ff9b::a2fa:7e13
rDNS record for 162.250.126.19: stfpanama.com
Not shown: 931 filtered tcp ports (no-response), 57 closed tcp ports (reset)
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp       Pure-FTPd
22/tcp   open  ssh       OpenSSH 7.4 (protocol 2.0)
53/tcp   open  domain    PowerDNS Authoritative Server 4.7.3
80/tcp   open  http      LiteSpeed
110/tcp  open  pop3      Dovecot pop3d
143/tcp  open  imap      Dovecot imapd
443/tcp  open  ssl/https LiteSpeed
465/tcp  open  ssl/smtp  Exim smtpd 4.96
587/tcp  open  smtp      Exim smtpd 4.96
993/tcp  open  ssl/imap  Dovecot imapd
995/tcp  open  ssl/pop3  Dovecot pop3d
3306/tcp open  mysql     MySQL 5.5.5-10.3.39-MariaDB-cll-lve
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.or
```

Directory and File Structure: I have created a file from UNISCAN tool and find this report. This file is /usr/share/uniscan/report/senselearner.com.html. Here some information are scan time started, target, scan time finished.



SCAN TIME

Scan Started: 27/9/2023 2:42:43

TARGET

Domain http://senselearner.com/

Server Banner: LiteSpeed

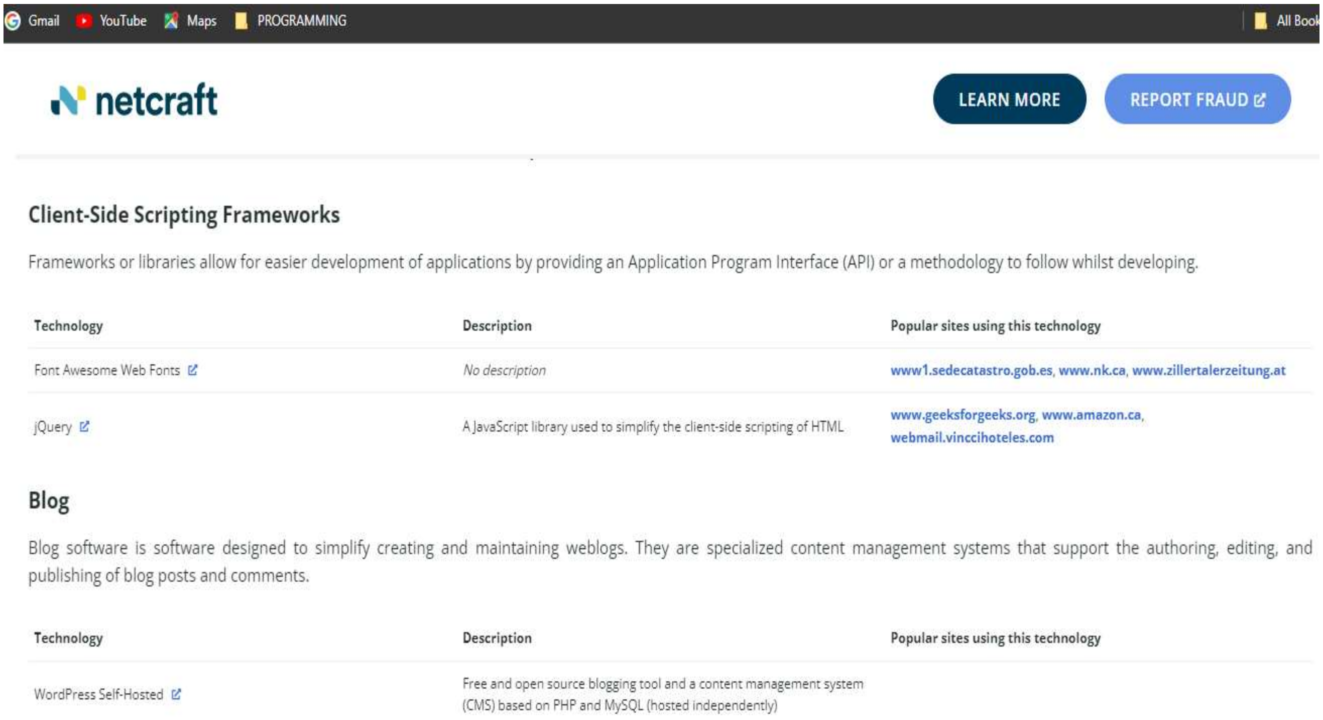
Target IP: 162.250.126.19

CRAWLING

SCAN TIME

Scan Finished: 27/9/2023 2:48:17

Technologies in Use: Here, All Lists content management systems (CMS), frameworks, or scripting languages used are jQuery, WordPress etc.



Client-Side Scripting Frameworks

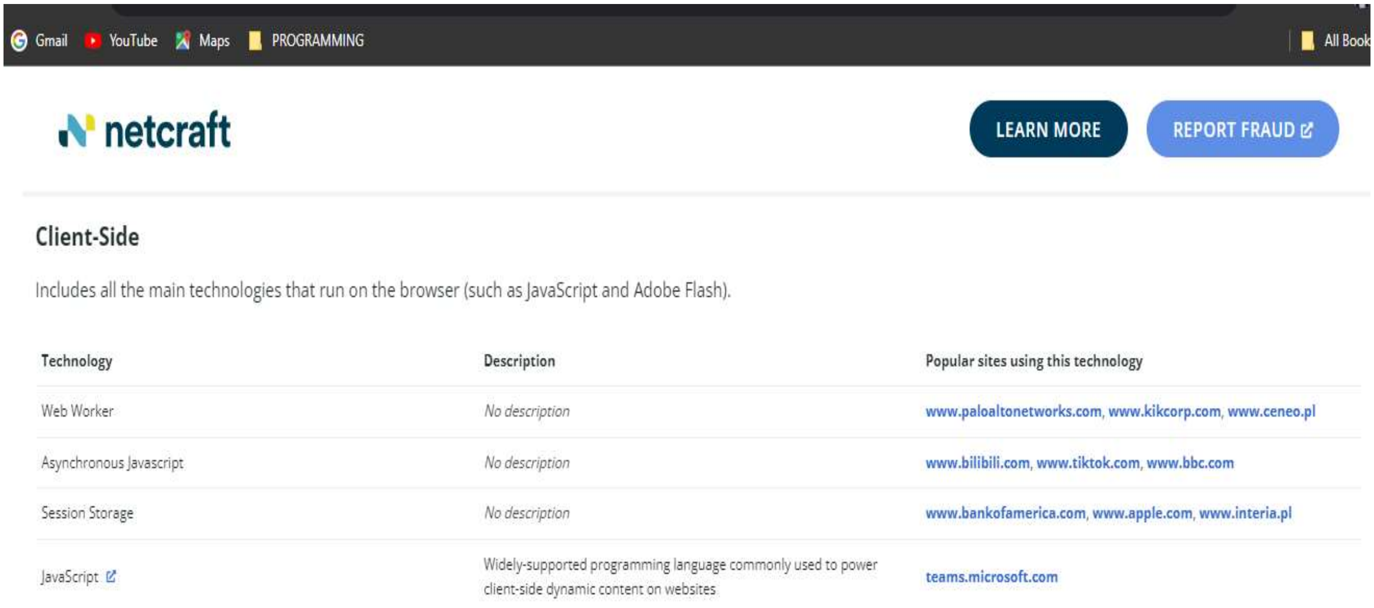
Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
Font Awesome Web Fonts	*No description*	www1.sedecatastro.gob.es, www.nk.ca, www.zillertalerzeitung.at
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.geeksforgeeks.org, www.amazon.ca, webmail.vinccihoteles.com

Blog

Blog software is software designed to simplify creating and maintaining weblogs. They are specialized content management systems that support the authoring, editing, and publishing of blog posts and comments.

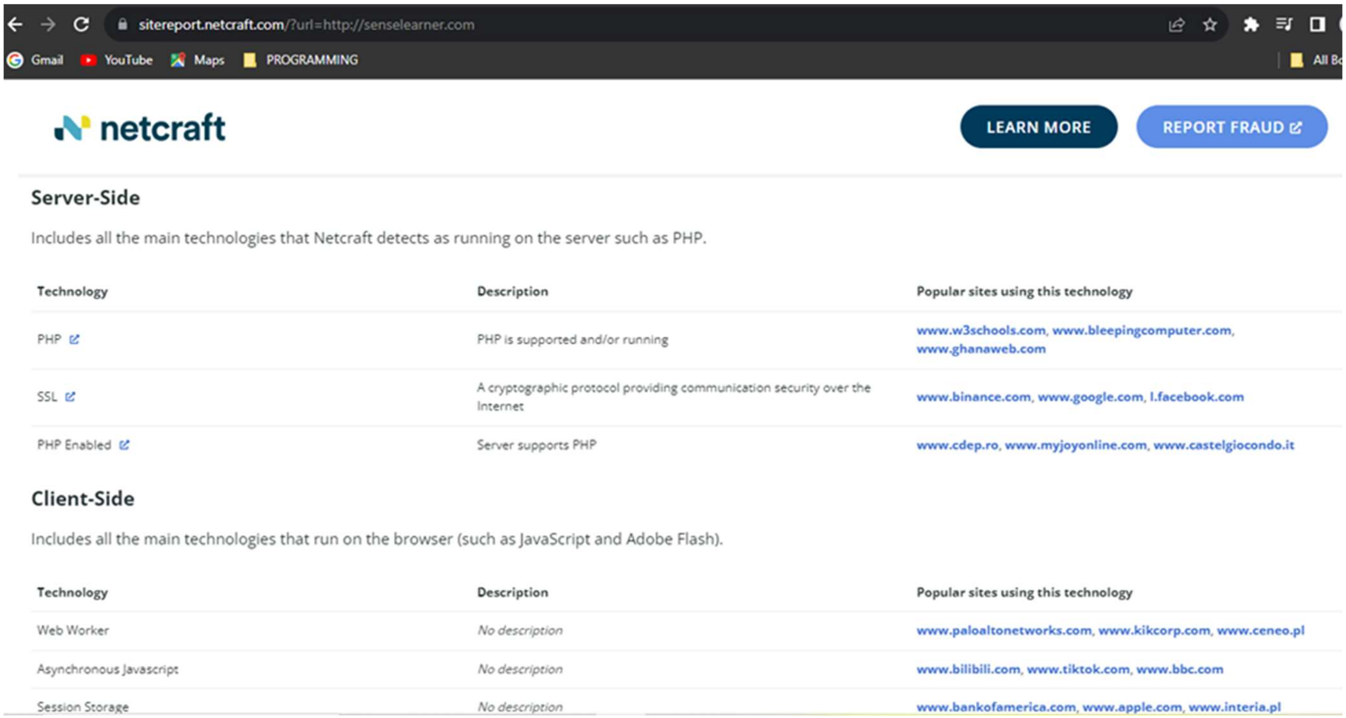
Technology	Description	Popular sites using this technology
WordPress Self-Hosted	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL (hosted independently)	



Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Web Worker	*No description*	www.paloaltonetworks.com, www.kikcorp.com, www.ceneo.pl
Asynchronous Javascript	*No description*	www.bilibili.com, www.tiktok.com, www.bbc.com
Session Storage	*No description*	www.bankofamerica.com, www.apple.com, www.interia.pl
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	teams.microsoft.com



Server-Side

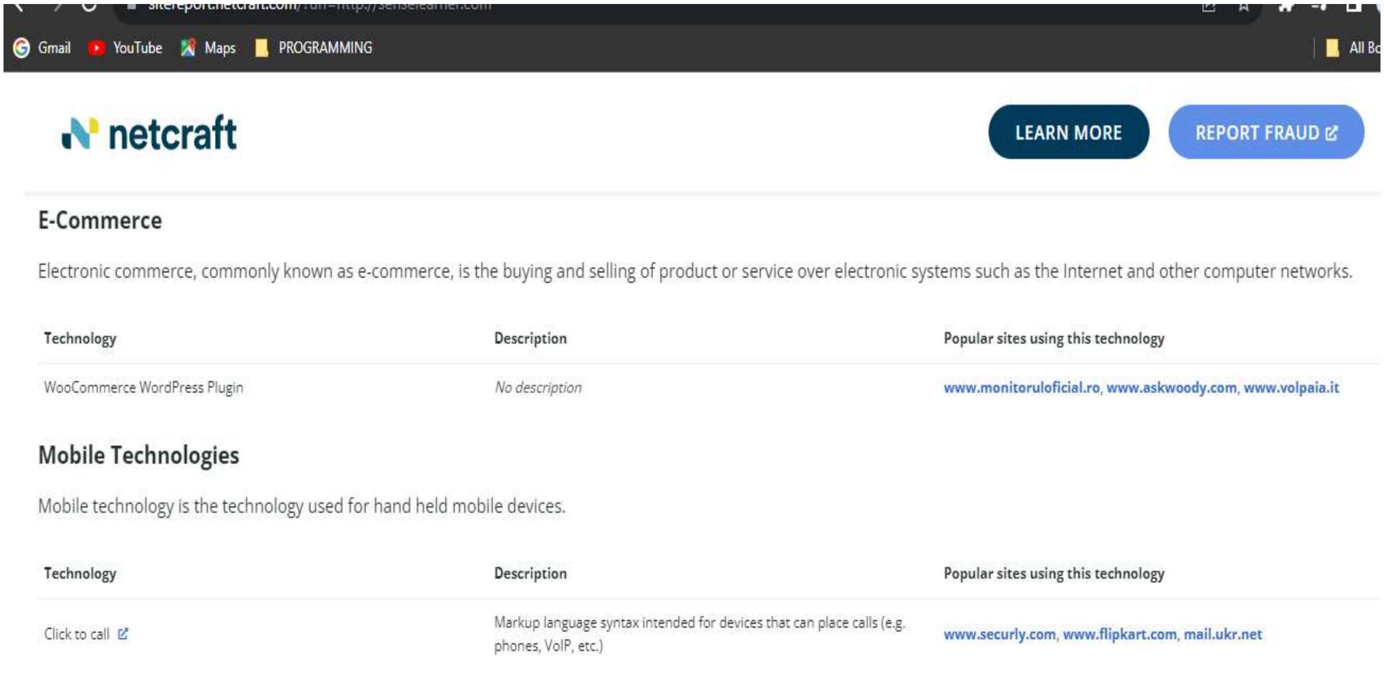
Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP	PHP is supported and/or running	www.w3schools.com, www.bleepingcomputer.com, www.ghanaweb.com
SSL	A cryptographic protocol providing communication security over the Internet	www.binance.com, www.google.com, l.facebook.com
PHP Enabled	Server supports PHP	www.cdep.ro, www.myjoyonline.com, www.castelgiocondo.it

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Web Worker	*No description*	www.paloaltonetworks.com, www.kikcorp.com, www.ceneo.pl
Asynchronous Javascript	*No description*	www.bilibili.com, www.tiktok.com, www.bbc.com
Session Storage	*No description*	www.bankofamerica.com, www.apple.com, www.interia.pl



E-Commerce

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the Internet and other computer networks.

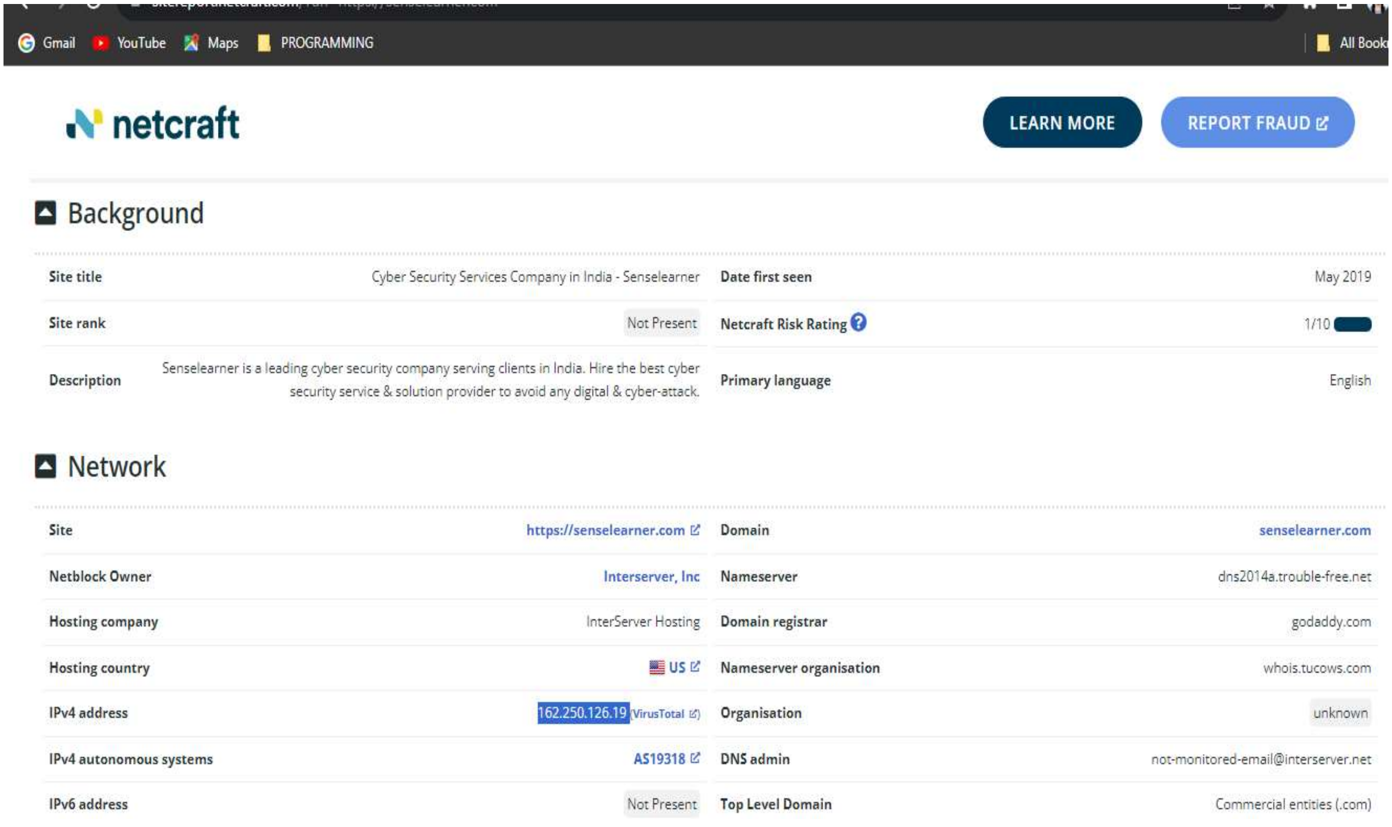
Technology	Description	Popular sites using this technology
WooCommerce WordPress Plugin	*No description*	www.monitoruloficial.ro, www.askwoody.com, www.volpaia.it

Mobile Technologies

Mobile technology is the technology used for hand held mobile devices.

Technology	Description	Popular sites using this technology
Click to call	Markup language syntax intended for devices that can place calls (e.g. phones, VoIP, etc.)	www.securly.com, www.flipkart.com, mail.ukr.net

Metadata: We find the metadata from net craft tools. All information are there like background, technology, client-side, server-side frameworks, SSL etc.

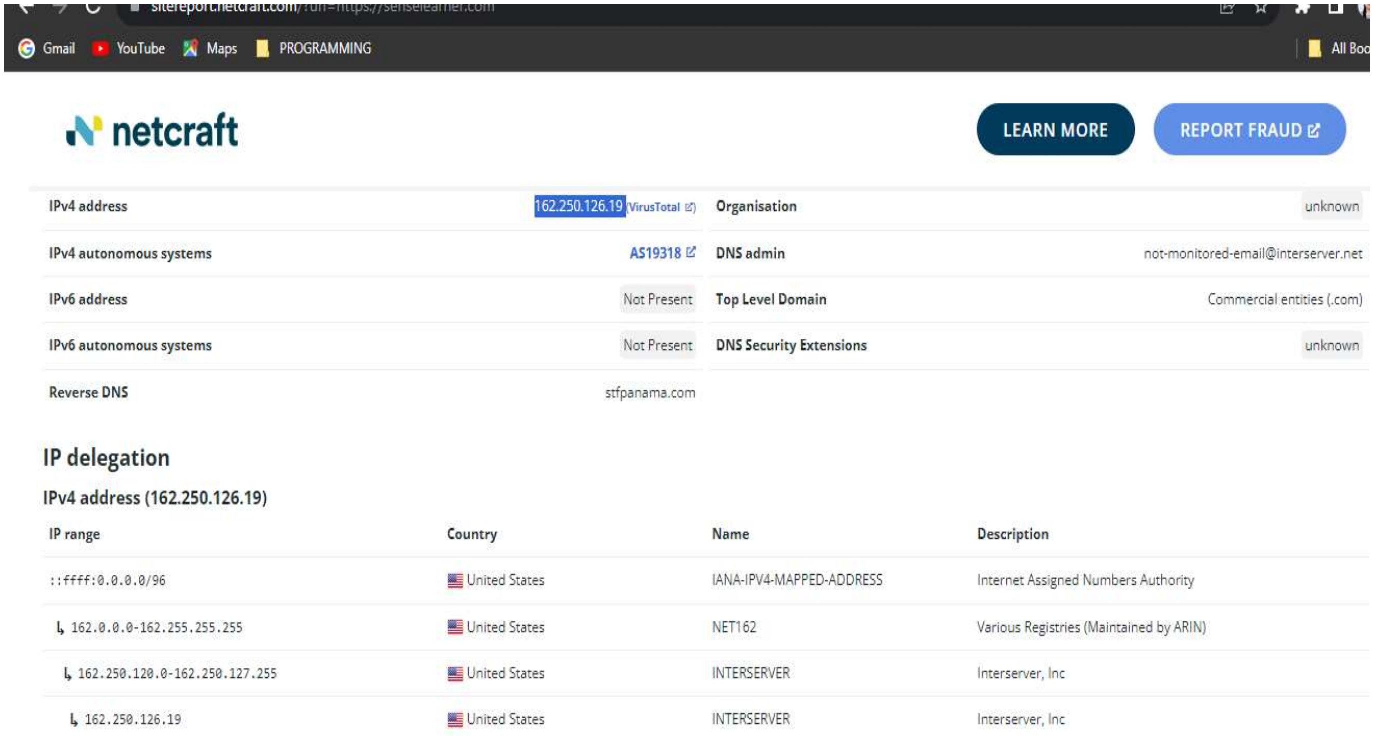


Background

Site title	Cyber Security Services Company in India - Senselearner	Date first seen	May 2019
Site rank	Not Present	Netcraft Risk Rating	1/10
Description	Senselearner is a leading cyber security company serving clients in India. Hire the best cyber security service & solution provider to avoid any digital & cyber-attack.	Primary language	English

Network

Site	https://senselearner.com	Domain	senselearner.com
Netblock Owner	Interserver, Inc	Nameserver	dns2014a.trouble-free.net
Hosting company	InterServer Hosting	Domain registrar	godaddy.com
Hosting country	US	Nameserver organisation	whois.tucows.com
IPv4 address	162.250.126.19 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS19318	DNS admin	not-monitored-email@interserver.net
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)

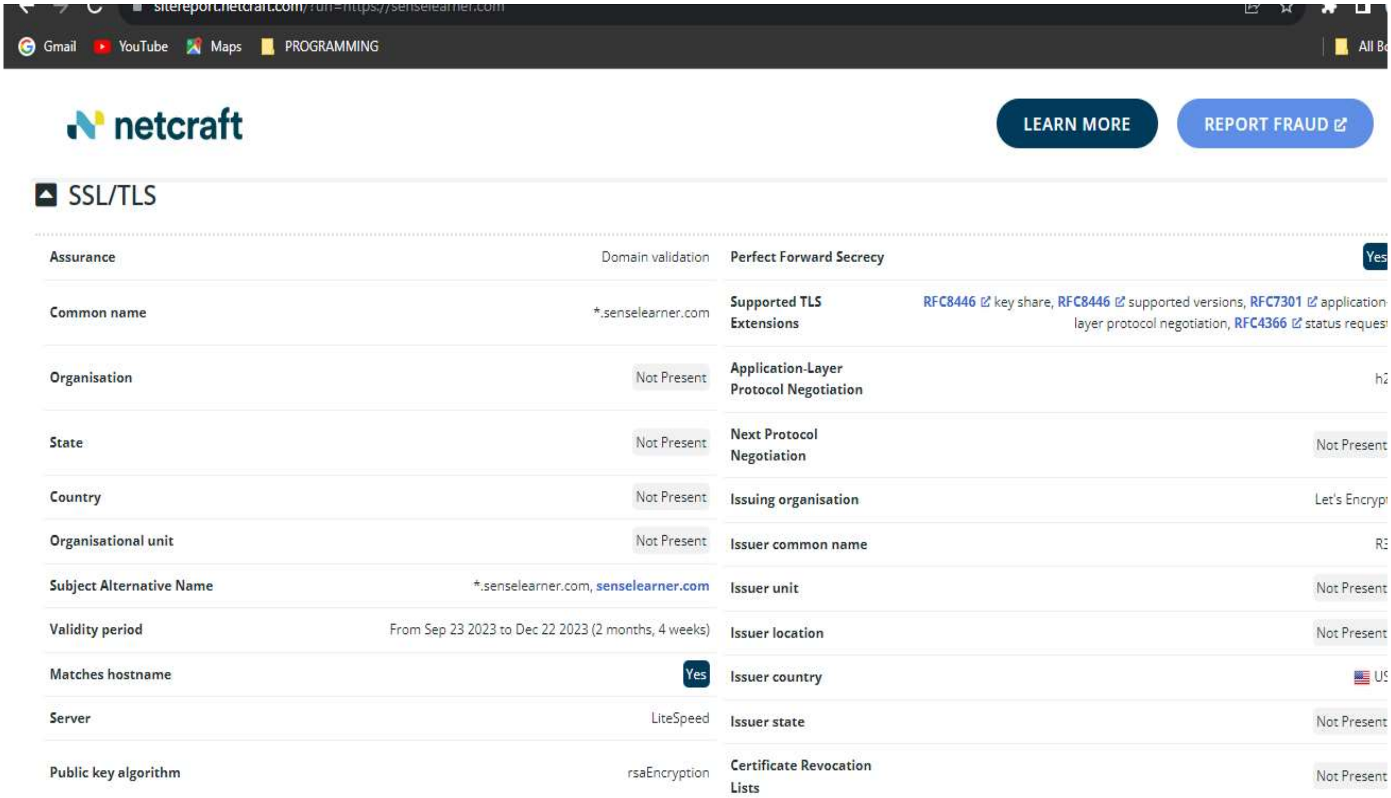


IPv4 address	162.250.126.19 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS19318	DNS admin	not-monitored-email@interserver.net
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	stfpanama.com		

IP delegation

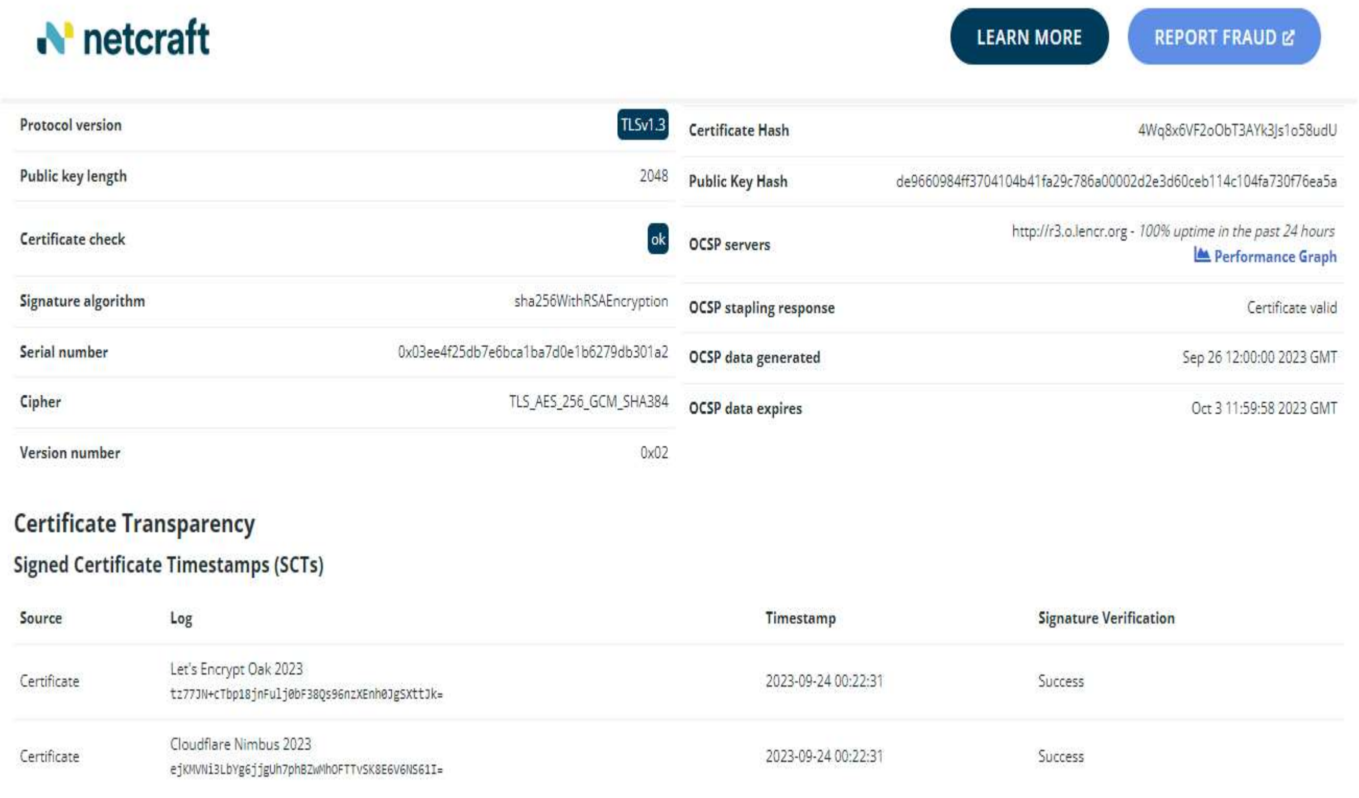
IPv4 address (162.250.126.19)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 162.0.0.0-162.255.255.255	United States	NET162	Various Registries (Maintained by ARIN)
↳ 162.250.120.0-162.250.127.255	United States	INTERSERVER	Interserver, Inc
↳ 162.250.126.19	United States	INTERSERVER	Interserver, Inc



SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	*.senselearner.com	Supported TLS Extensions	RFC8446 key share, RFC8446 supported versions, RFC7301 application-layer protocol negotiation, RFC4366 status request
Organisation	Not Present	Application-Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	Let's Encrypt
Organisational unit	Not Present	Issuer common name	R3
Subject Alternative Name	*.senselearner.com, senselearner.com	Issuer unit	Not Present
Validity period	From Sep 23 2023 to Dec 22 2023 (2 months, 4 weeks)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	LiteSpeed	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	Not Present



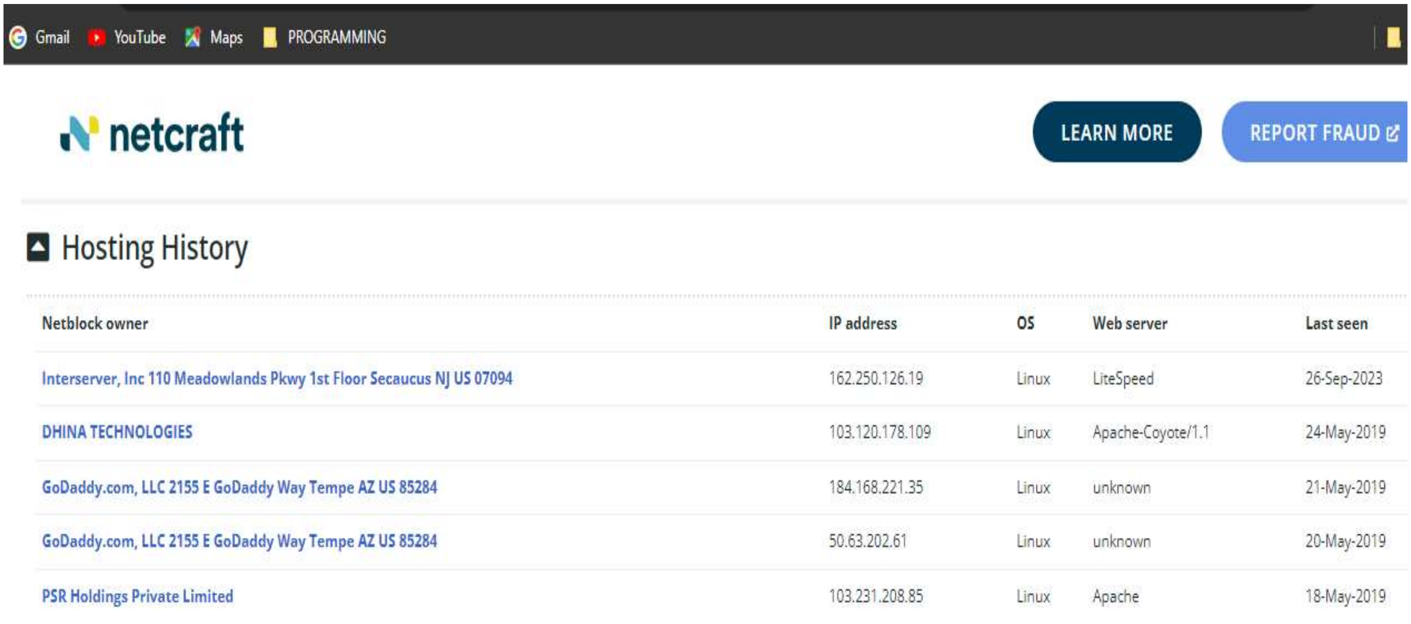
Protocol version	TLSv1.3
Public key length	2048
Certificate check	ok
Signature algorithm	sha256WithRSAEncryption
Serial number	0x03ee4f25db7e6bca1ba7d0e1b6279db301a2
Cipher	TLS_AES_256_GCM_SHA384
Version number	0x02

Certificate Hash	4Wq8x6VF2oObT3AYk3Js1o58udU
Public Key Hash	de9660984ff3704104b41fa29c786a00002d2e3d60ceb114c104fa730f76ea5a
OCSP servers	http://r3.o.lencr.org - *100% uptime in the past 24 hours* Performance Graph
OCSP stapling response	Certificate valid
OCSP data generated	Sep 26 12:00:00 2023 GMT
OCSP data expires	Oct 3 11:59:58 2023 GMT

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Let's Encrypt Oak 2023 `tz77JN+cTbp18jnFulj0bF38Qs96nzXEnh0JgSXttJk=`	2023-09-24 00:22:31	Success
Certificate	Cloudflare Nimbus 2023 `ejKMVNi3LbYg6jjgUh7phBZwMhOFTTvSK8E6V6NS61I=`	2023-09-24 00:22:31	Success



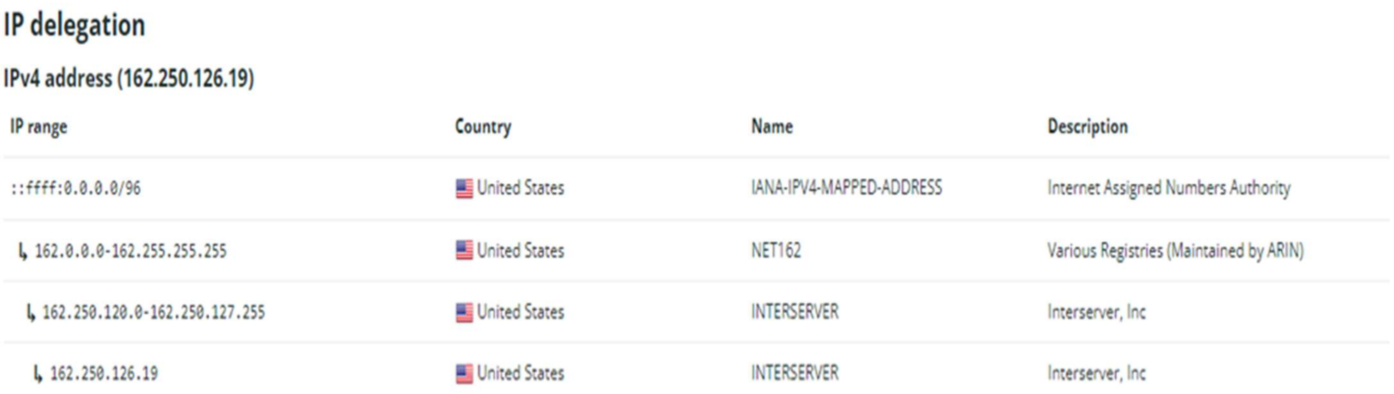
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Interserver, Inc 110 Meadowlands Pkwy 1st Floor Secaucus NJ US 07094	162.250.126.19	Linux	LiteSpeed	26-Sep-2023
DHINA TECHNOLOGIES	103.120.178.109	Linux	Apache-Coyote/1.1	24-May-2019
GoDaddy.com, LLC 2155 E GoDaddy Way Tempe AZ US 85284	184.168.221.35	Linux	unknown	21-May-2019
GoDaddy.com, LLC 2155 E GoDaddy Way Tempe AZ US 85284	50.63.202.61	Linux	unknown	20-May-2019
PSR Holdings Private Limited	103.231.208.85	Linux	Apache	18-May-2019

Network and WHOIS Enumeration:

Discuss network and WHOIS enumeration results:

Network Range: Find the network range, IP addresses and also country with description.

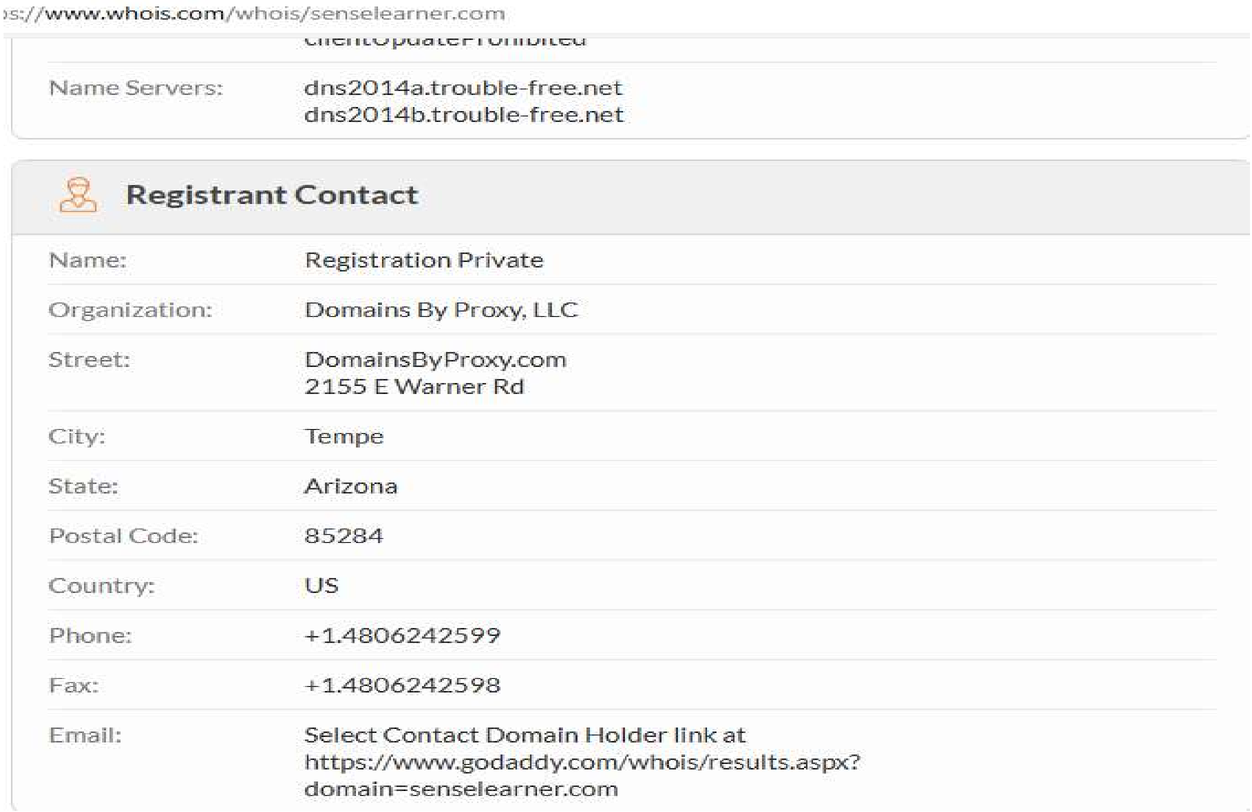


IP delegation

IPv4 address (162.250.126.19)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 162.0.0.0-162.255.255.255	United States	NET162	Various Registries (Maintained by ARIN)
↳ 162.250.120.0-162.250.127.255	United States	INTERSERVER	Interserver, Inc
↳ 162.250.126.19	United States	INTERSERVER	Interserver, Inc

WHOIS Records: Include details from WHOIS records, such as the registrant's contact information.



s://www.whois.com/whois/senselearner.com

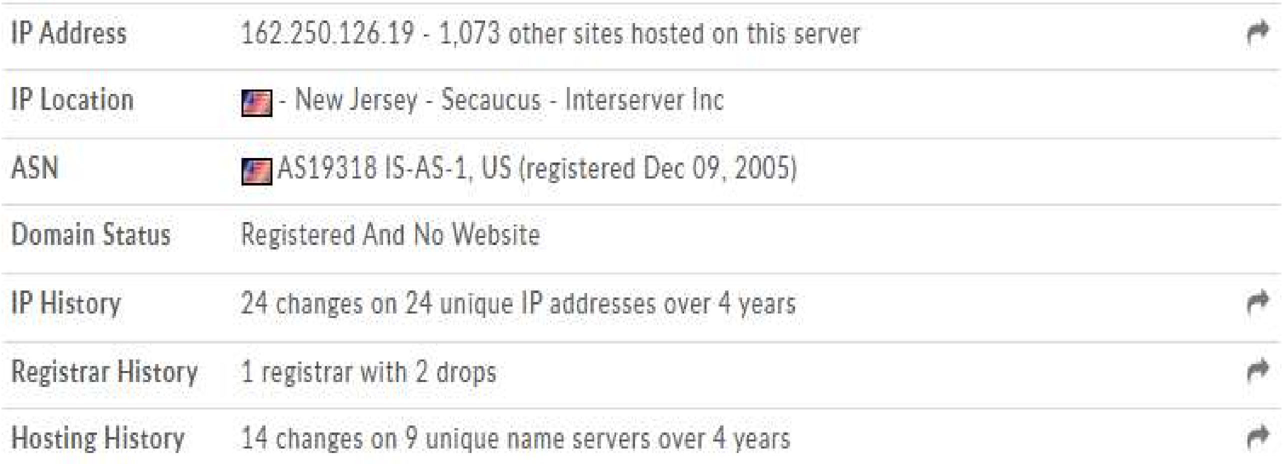
clientUpdateProhibited

Name Servers:	dns2014a.trouble-free.net dns2014b.trouble-free.net

Registrant Contact

Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd
City:	Tempe
State:	Arizona
Postal Code:	85284
Country:	US
Phone:	+1.4806242599
Fax:	+1.4806242598
Email:	Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=senselearner.com

ASN Information: If applicable, mention Autonomous System Number (ASN) data.



IP Address	162.250.126.19 - 1,073 other sites hosted on this server
IP Location	- New Jersey - Secaucus - Interserver Inc
ASN	AS19318 IS-AS-1, US (registered Dec 09, 2005)
Domain Status	Registered And No Website
IP History	24 changes on 24 unique IP addresses over 4 years
Registrar History	1 registrar with 2 drops
Hosting History	14 changes on 9 unique name servers over 4 years

Open-Source Intelligence (OSINT)

1.Whois Data: The Whois tool provided registration information about the target domain, including details about the domain owner, registrar, and registration date. This information can be used to understand the entity behind the website.

2.Netcraft: Netcraft likely provided insights into the web server technology and hosting provider used by the target website. This can be valuable for understanding potential vulnerabilities associated with the server technology.

3.CentralOps: CentralOps is a versatile tool that can provide various insights, including DNS and network-related information. It may have revealed DNS records, IP address details, and other network-related data.

4.Uniscan: Uniscan, as mentioned earlier, was used for web application scanning. While its primary purpose is vulnerability scanning, it may have identified certain elements of the web application and potential security concerns.

5. Nmap: Nmap, a network scanning tool, may have been used to identify open ports and services on the target server. This can be useful for understanding the attack surface and potential points of entry.

6.Subdomain Finder: This tool likely assisted in identifying subdomains associated with the target domain. Subdomains can be significant as they may host different web applications or services.

Incorporate the specific findings from these tools into your OSINT summary. For example:

1.Web Server Technology: Netcraft revealed that the website is hosted on a specific web server technology (e.g., Apache, Nginx), which is valuable information for assessing potential vulnerabilities associated with that technology.

2.Subdomains: The subdomain finder tool identified several subdomains associated with the target domain. These subdomains can be potential entry points for attackers or may host different web applications.

3.Network Details: Information from CentralOps and Nmap may have provided details about the target's network infrastructure, such as IP addresses and open ports, which is critical for understanding the network's security posture.

4.Vulnerabilities: Uniscan may have highlighted potential vulnerabilities in the web application, which should be further investigated as part of the cybersecurity assessment.

Vulnerabilities and Security Concerns :

Open Ports and Services Enumeration:

During the information gathering phase, the assessment team successfully identified open ports and their associated services on the target network. The following vulnerabilities were discovered in this context:

a. Open Port Enumeration: Several open ports were identified on the target server. These open ports represent potential entry points for attackers and can be considered security vulnerabilities.

b. Service and Version Detection: In addition to identifying open ports, the assessment team also determined the service running on each open port along with its version number. This information is crucial for understanding the attack surface and potential vulnerabilities associated with specific service versions.

These findings provide a starting point for further analysis and vulnerability assessment. The next steps in the assessment process should involve in-depth vulnerability scanning and testing of these services and versions to identify and mitigate potential security weaknesses.

The open ports are given in web foot printing task of web information ghathering using nmap please refer this.

Recommendations :

Regular Vulnerability Scanning and Patch Management:

Implement a routine vulnerability scanning process using specialized tools to detect and assess vulnerabilities in the open ports and services.

Establish a patch management procedure to ensure that all software and services, especially those with known vulnerabilities, are kept up to date with the latest security patches.

Service Version Updates:

For services with identified versions, update them to the latest stable releases. This will often include security fixes and enhancements.

Minimize Open Ports:

Review and assess the necessity of each open port and service. Close any ports or services that are not required for the organization's operations to minimize the attack surface.

Access Control and Firewall Rules:

Implement robust access control policies and firewall rules to restrict access to open ports and services only to authorized users or systems. Limit external exposure as much as possible.

Security Configuration Review:

Conduct a comprehensive review of the security configurations of open ports and services. Ensure that security features and best practices, such as strong encryption, authentication mechanisms, and access controls, are correctly implemented.

Penetration Testing:

Consider conducting penetration testing to simulate real-world attacks on your systems. This can help identify potential weaknesses that may not be apparent through vulnerability scanning alone.

Data Encryption:

Enable encryption for sensitive data transmitted over open ports and services, especially when handling personally identifiable information (PII) or confidential data.

Implement Intrusion Detection and Prevention Systems (IDPS):

Deploy IDPS solutions to monitor network traffic and detect and respond to suspicious activities or intrusion attempts in real-time.

Employee Training and Awareness:

Provide cybersecurity training to employees to enhance their awareness of security best practices, including identifying phishing attempts and maintaining strong password hygiene.

Backup and Disaster Recovery Plan:

Establish and maintain regular data backups, and implement a disaster recovery plan to ensure data availability and business continuity in the event of a security incident.

Incident Response Plan:

Develop a well-defined incident response plan that outlines procedures to follow in case of a security breach or incident. Ensure that all employees are aware of the plan and their roles in it.

Regular Security Audits:

Conduct periodic security audits and assessments to evaluate the effectiveness of security measures and identify any emerging threats or vulnerabilities.

Compliance with Security Standards:

Ensure compliance with industry-specific security standards and regulations, such as GDPR, HIPAA, or ISO 27001, where applicable.

Conclusion:

In conclusion, the information gathering and preliminary assessment conducted on the target organization's digital presence have provided valuable insights into its cybersecurity posture and potential areas of concern. This comprehensive assessment aimed to evaluate the organization's security from various angles, including domain information, DNS footprinting, web footprinting, network and WHOIS enumeration, open-source intelligence (OSINT), and the identification of vulnerabilities and security concerns.

Throughout the assessment, several key findings and vulnerabilities were identified:

1.The enumeration of open ports and associated services, along with their versions, revealed potential entry points and areas of focus for further security analysis.

These findings serve as a starting point for enhancing the organization's cybersecurity measures and mitigating potential risks. It is imperative for the organization to take proactive steps to address these vulnerabilities and strengthen its overall security posture.

To this end, the following actions are recommended:

- **Implement a regular vulnerability scanning and patch management program to keep software and services up to date.**

- **Update service versions to the latest stable releases to ensure the inclusion of security fixes.**
- **Minimize open ports and services to reduce the attack surface.**
- **Enhance access control and firewall rules to restrict unauthorized access.**
- **Review and enhance security configurations for open ports and services.**
- **Consider conducting penetration testing to identify additional weaknesses.**
- **Encrypt sensitive data transmitted over open ports and services.**
- **Deploy Intrusion Detection and Prevention Systems (IDPS) for real-time monitoring.**
- **Provide cybersecurity training to employees to enhance awareness and security practices.**
- **Establish and maintain data backups and a disaster recovery plan.**
- **Develop and regularly update an incident response plan.**
- **Ensure compliance with industry-specific security standards and regulations.**

By addressing these recommendations and maintaining a proactive and vigilant approach to cybersecurity, the organization can significantly reduce its exposure to potential threats and bolster its resilience against cyberattacks.

It is important to note that cybersecurity is an ongoing process, and regular assessments, monitoring, and updates are essential to stay ahead of evolving threats and vulnerabilities. The organization should remain committed to its security efforts and adapt to the changing cybersecurity landscape to protect its digital assets and maintain the trust of its stakeholders.

Appendices :

I have added already in each tasks steps kindly refer that screenshots.

References

List all the sources and tools used during the information gathering process.

- **https://www.whois.com/**
- **https://whois.domaintools.com/**
- Free online network tools - traceroute, nslookup, dig, whois lookup, ping - IPv6 (centralops.net)
- **https://www.netcraft.com/tools/**
- **https://subdomainfinder.c99.nl/**